NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

AN INTEGRATED ARCHITECTURE TO SUPPORT HASTILY FORMED NETWORK

by

Lim Meng Hwee
Ng Min Yew Calvin

December 2007

Thesis Co-Advisors:	Brian D. Steckler
	Gurminder Singh
Second Reader:	Scott Mckenzie

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No.
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** December 2007	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE: An Integrated Architecture to Support Hastily Formed Network (HFN)			**5. FUNDING NUMBERS**
6. AUTHOR(S) Lim Meng Hwee, Ng Min Yew Calvin			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			**12b. DISTRIBUTION CODE**
13. ABSTRACT (maximum 200 words) This thesis analyzes the nature of Hastily Formed Network (HFN) scenarios and develops framework and architecture for effective collaboration needs. It will entail a spectrum of COTS hardware (e.g. Mobile Command and Control (C2) center, communication networks) and software (e.g. resource optimizing tools), that could support a wider continuum of militants or Non-government Organization (NGOs) humanitarian and crisis relief missions, as well as ad-hoc anti-terrorist threat missions. Various phases of the disaster or incident will be studied and suitable information technologies will be identified and introduced to better the effectiveness and efficiency capabilities in the collaboration aspects of the operations.			
14. SUBJECT TERMS Hastily Formed Network (HFN), Wireless Deployment, Collaboration Tools			**15. NUMBER OF PAGES** 111
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

AN INTEGRATED ARCHITECTURE TO SUPPORT THE HASTILY FORMED NETWORK (HFN)

Meng Hwee Lim
Civilian, Singapore Technologies Engineering, Singapore
B.Eng., (Hons), University of Birmingham UK, 2003

Min Yew Calvin Ng
Civilian, Ministry of Defense, Singapore
B.Eng., (Hons), Nanyang Technological University, 1998

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN COMPUTER SCIENCE

from the

NAVAL POSTGRADUATE SCHOOL
December 2007

Authors: Meng Hwee Lim

Min Yew Calvin Ng

Approved by: Brian D Steckler
Co-Thesis Advisor

Gurminder Singh
Thesis Co-Advisor

Scott Mckenzie
Second Reader

Peter J. Denning
Chairman, Department of Computer Science

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This thesis analyzes the nature of Hastily Formed Networks (HFN) and develops a framework and architecture for effective collaboration needs. The analysis considers review of a spectrum of Commercial off-the-shelf (COTS) hardware (including Mobile Command and Control (C2) center and network hardware) and software (i.e., resource optimizing tools) that could support a wider continuum of humanitarian and crisis-relief missions as well as ad-hoc anti-terrorist threats missions. Military and Non-Governmental Organization (NGO) participation is considered. Various phases of disasters or incidents are studied and suitable Information and Communications Technologies (ICT) and capabilities are identified to improve the effectiveness and efficiency of collaborative operations.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ABBREVIATIONS AND ACRONYMS

ACRONYM	DEFINITION
AC	Alternating Current
AMP	Airwave Management Platform
AWMS	Airwave Wireless Management Suite
C2	Command and Control
COTS	Commercial off-the-shelf
DC	Direct Current
DHCP	Dynamic Host Configuration Protocol
DHS	Department of Homeland Security
DoD	Department of Defense
DSS	Decision Support Systems
FFA	Free-For-All
FLAK	FLy Away Kit
FOUO	For Official Use Only
GATR	Ground Antenna Transmit and Receive
GPS	Global Position System
HADR	Humanitarian Assistance and Disaster Relief
HCI	Human Computer Interface
HFN	Hastily Formed Network
HQ	Headquarters
HTTP	Hypertext Transmission Protocol
ICT	Information and Communications Technologies

ACRONYM	DEFINITION
IDS	Intrusion Detection System
IM	Instant Messaging
ISM	Industrial, Scientific and Medical
LA	Los Angeles
LACoFD	LA County Fire Department
LACoS	LA County Sheriff
LAN	Local Area Network
LOS	Line-of-sight
MAG46	Marine Aircraft Group 46
MAN	Metropolitan Area Network
MANET	Mobile Ad-hoc Network
MCP	Mobile Command Post
MMI	Man-Machine Interface
NGO	Non-Governmental Organization
NLOS	Non-line of sight
OSU	Outdoor Subscriber Unit
OGP	Operation Golden Phoenix
PAN	Personal Area Network
PDA	Personal Digital Assistant
QoS	Quality of Service
RAPIDS	Rogue AP Detection
RBAC	Role-Based Access Control
REBRO	Rebroadcast

ACRONYM	DEFINITION
RF	Radio Frequency
SA	Situation Awareness
SNMP	Simple Network Management Protocol
SOA	Service-Oriented Architecture
SWOT	Strengths, Weaknesses, Opportunities and Threat
UC	Unclassified
UCC	Unified Command Center
UHF	Ultra High Frequency
VHF	Very High Frequency
VoIP	Voice over Internet Protocol
WAN	Wide Area Network
WAP	Wireless Access Points
WEP	Wired Equivalent Privacy
WiFi	Wireless Fidelity
WiMAX	Worldwide Interoperability for Microwave Access
WPA	WiFi Protected Access
WYSIWYG	What You See Is What You Get

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

We would like to express thanks to many individuals who have influenced and assisted us during the development of this thesis.

We would like to express thanks to many individuals who have influenced and assisted us during the development of this thesis.

Thanks to our thesis supervisors, Prof. Brian D. Steckler and Prof. Gurminder Singh for their valuable advice and guidance. We believe that the knowledge they have imparted to us will benefit us in our future endeavors.

Thanks to Scott McKenzie for his help in editing our thesis.

Thanks to Prof. Steckler again and to Lt Col Carl Oros for giving us the opportunity to deploy alongside the troops in Operation Golden Phoenix 07. It has been a great experience for us.

We also wish to thank our sponsor, the Defence Science and Technology Agency (DSTA) and Singapore Technologies Engineering (STE) for enabling and supporting our participation in this valuable program at the Naval Postgraduate School.

Last but not least, thanks to our families and friends here in Monterey and in Singapore for their moral support. It is their encouragement that keeps us going,

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. THESIS STATEMENT

This thesis analyzes the dynamic nature of Hastily Formed Networks (HFN) and develops the architecture required for effective collaboration. It will entail review of a spectrum of Commercial off-the-shelf (COTS) hardware (e.g., mobile devices, mobile command center equipment, and communications network equipment) and software (e.g., resource optimizing tools) that could support a wide continuum of first-responders from the Department of Homeland Security (DHS,) Local and State Governments, or Non-Governmental Organization (NGO) in the performance of Humanitarian Assistance and Disaster Relief (HA/DR) missions. Various phases of the disaster or incident will be studied, including the opportunity to conduct field experimentation in Operation Golden Phoenix (OGP) 2007. Based on the observation data collected in OGP and other real and simulated scenarios, suitable Information Communication Technologies (ICT) will be identified for their value to improvement of the effectiveness and efficiency of HFN operations.

B. THESIS SCOPE AND OBJECTIVES

This thesis is conducted in support of the DHS in its effort to:

- evaluate existing ICT deployed during HA/DR scenarios, and
- propose integrated information system architectures to support HFN.

This thesis will address the gaps in current systems, focusing on collaboration and interoperability of the systems.

The student team participated in OGP 2007 to collect empirical data for analysis and study, focusing on the collaboration issues between military and civilian agencies (otherwise known as "Civ-Mil Boundary" issues.) A field report has been consolidated and analyzed as part of the thesis report.

A spectrum of relevant COTS ICT will be recommended. The impact of this research could benefit future Department of Defense (DoD) and DHS HA/DR operations.

This thesis is comprised of the following chapters:

1. Chapter I – Introduction

This chapter provides the thesis statement and defines the scope of the thesis. It gives an overview of the chapters and annexes to this work.

2. Chapter II – Background

This chapter provides a literature review on HFN, discusses current technologies used to support HFN activities, provides an introduction to OGP, and offers a discussion on the methodology to approach the experimentation and collect empirical observations.

3. Chapter III – Operational Analysis of HFN

This chapter provides an analysis of the dynamics of HFN scenarios, and introduces observation data collected in OGP. Subsequently, it identifies the collaboration needs and current gaps to support our recommendations.

4. Chapter IV- Integrated Information System Architecture

This chapter discusses the proposed architecture to support the dynamic nature of HFN operations.

5. Chapter V – Proposed Technology Implementation

This chapter suggests an implementation approach and discusses a spectrum of COTS ICT that could augment HA/DR missions with a more effective and efficient collaborative environment. It also embraces the needs and conforms to the proposed architecture (suggested in the earlier chapters) required to address the interoperability among the diverse participants.

6. Chapter VI – Conclusion

This chapter summarizes the work accomplished in this thesis and offers proposals for future research.

II. BACKGROUND

A. HFN

The main purpose of HFN is to allow people to be networked and to share information. Disasters in recent years such as the Southeast Asia Tsunami, Hurricane Katrina, and the September. 11 attack have reiterated the importance of communication in these scenarios. Sharing information in the aftermath, in the form of voice, data and video, will provide search and rescue mission planners with situation awareness and information superiority needed for in-depth understanding of operation needs. These cannot be made possible without communication. Without formal communications, command and control over the mobile forces would be inefficient. Coordination work, such as air drops of medical and food supplies, can be tedious and more time is required to facilitate these activities. With these barriers, Humanitarian Assistance and Disaster Relief (HA/DR) missions will become an uphill task, which means more life and assets might be lost as a result.

HFNs can be put together using a suite of COTS wireless gears, such as satellite communication, Wireless Fidelity (WiFi) and Worldwide Interoperability for Microwave Access (WiMAX), to provide communication for the disasters hit areas. The equipment is designed to be easy to use and portable. These characteristics are essential to make HFNs suitable for deployment in disasters since the required expertise to setup complicated equipment and road infrastructure to transport large bulky equipment may not be available.

B. AN INTEGRATED INFORMATION SYSTEM ARCHITECTURE

The demand for support of a myriad of operations has fostered the requirement to put together a spectrum of new systems or new ways of doing things that are able to meet the ever-changing needs with more effectiveness. COTS equipment embedded with the most advanced technologies are widely available.

However, an integrated architecture that allows the interoperability of these individual systems and the execution of the best practices does not exist. Therefore, it is vital to have a reliable framework to govern the flow of these disparate activities.

C. GOLDEN PHOENIX

In July, 2007, OGP [Appendix A] provided an avenue for experimentation and observation of a simulated DR scenario, and became the basis for this thesis. By nature, OGP is a collaborative training event. It is designed to allow participants from the local, regional, state, and federal agencies to become familiar with the procedures and policies that are in place should disaster (man-made or natural) strike.

Participants on the ground were our main source for discovering the actual requirements of HFNs. Observing the participants in real-time facilitated our understanding of the communications limitations that exist and inhibit efficient HA/DR operations. It is through observing human behavior and actions that we can establish the requirements for systems that would help them perform better.

1. The Methodologies

During the exercises, a series of techniques were adopted to discover the requirements of HFNs.

a. Observing the Participants – Direct Observation

Direct observation is a straightforward method that allows for rapid results with an insight into the participants, their tasks, and their environments. It can be undertaken in the form of either field studies or controlled studies. Field studies directly observe participants in their normal work, such as the deployment areas, or in their command vehicles doing their routine work, with the observer taking notes on any interesting behaviors. Controlled studies observe participants in a confined area other than a normal working environment, such as a network room, performing specific tasks with the observer taking note of their performance, specifically their familiarity with the usability of the system and their physical handling of the system.

b. Interviewing the Participants

Interviewing involves talking to and/or questioning the participants. It enables the gathering of information in a fast and friendly way. It is of paramount importance to structure interviews carefully, deciding in advance who to interview, what questions to ask to gather the required information, and the duration of the interviews. There are two kinds of interviews: the structured and unstructured. A structured interview provides a set of predetermined questions. The whole interview session will follow the flow of the predetermined questions. There is little or no possibility that additional topics will be brought up by the interviewer during the conduct of the interview. The unstructured interview, a more flexible method, also has a predetermined set of topics for discussion and exploration. However, there is no fixed sequence of how the questions will be asked; instead the interviewer will react according to how the participants reply. The interviewer is allowed to probe further if they want to find out more.

c. Questionnaires

Questionnaires take a more rigid approach to the data collection requirement. A set of questions is prepared for the collection of more precise information. There are two question structures for questionnaires: closed and open. Closed questions provide the respondent with a predefined type of answer for every question, such as a rating scale of one to five, with the extremes being rated as one for "don't agree" and five for "totally agree" or just "yes" or "no" replies. This approach for collecting information is easy to analyze since the requirement is to count the number of responses in each category. Open questions allow the respondent to answer however they like. This form of information collection technique allows the collection of more data. On the other hand, it is more time-consuming to analyze data for open questions than for closed questions.

D. SUMMARY

This chapter has provided an overview of HFN and the requirement to formulate an integrated architecture to support its operation. A short overview of OGP and the

methodologies adopted during OGP for the gathering requirements, and the experiments conducted to support this thesis, were also explained.

III. OPERATIONAL ANALYSIS OF HFN SCENARIO

Analysis of the various past HFN scenarios has provided us with good insight into the dynamics of each scenario and into how, in general, first-responders (first-responders are the emergency personnel that were called to the scene of crisis such as fire fighters, police officers, sheriff and medical services professionals) react. In this chapter, we will examine various types of HFN scenarios to understand the characteristics and needs of the situation, and to facilitate the design of an integrated communications architecture and framework to effectively support HA/DR missions. Past scenarios to be referenced include the September 11 World Trade Center attack, the December 2004 Indian Ocean Tsunami, and the August 2005 Hurricane Katrina.

We have also included our OGP participation into the analysis. OGP was conducted in Los Angeles (LA) County to examine the current state of ICT development and the collaborative natures of the participating organizations. OGP was held July 16–26, 2007. It simulated an 8.0 earthquake scenario in LA County. Participants from local, regional, state, and federal entities were involved. In particular, the participants were involved in an experiment that required the collaboration of civil and military agencies in order to exercise California state and federal disaster relief protocols. Lead agencies included the LA County Sheriff (LACoS), the LA County Fire Department (LACoFD), and the Marine Aircraft Group 46 (MAG46.)

A. DYNAMICS OF HFN SCENARIO

The dynamics of the HFN scenario are a key point of study in determining the right architecture for an effective and efficient HFN. The dynamics of the HFN scenario are dependent on the relationship between the cause and effect of the scenario. The need for HFNs can arise from three main scenario types: known, unsure and unknown. Table 1 lists the categories and their related characteristics.

Nature of Cause	Characteristic	Examples
Known	Expected events Planned and ready to execute	Fire fighting incident, forest fire
Unsure	Not sure what to do More time and resource will ease understanding	Hurricane Katrina happened with some expectation but the impact was unknown.
Unknown	"Surprise" element—caught off guard Unknown way to handle Outcome unknown Chaos	Sept 11 attack and Indian Ocean tsunami

Table 1. Scenario of HFN Based on Nature of Cause [After 3]

1. The known

The cause of the scenario is well understood and within control. The response team knows what to do and how to accomplish the mission. Examples include fire fighting and forest fire scenarios.

2. The Unsure

The cause of the scenario is unsure. Responders will have some difficulty understanding the event. However, given sufficient time and resources, understanding can take place.

3. The Unknown

The cause of the scenario is unknown. The event has an element of "surprise" with no definite concluding understanding. Responders have to react spontaneously and instantaneously.

On the elements of effects, the disaster scenario will cause devastating effects to humanity and infrastructure over a range of magnitudes. In the case of the September 11 attack, the magnitude of the infrastructure devastated resulted in an economic impact that amounted to $1.2 trillion and the deaths of 2,749. On other end, a tsunami over the Indian Ocean resulted in a massive wave that killed large numbers of people residing along the coastline of South and Southeast Asia—a death toll estimated to be over 230,000.

The dynamics of an HFN scenario can be illustrated in Figure 1. The illustration shows that with increasing unknown cause and magnitude of events, the dynamic relationship between cause and effect transit from a state of order, to complexity, to chaos.

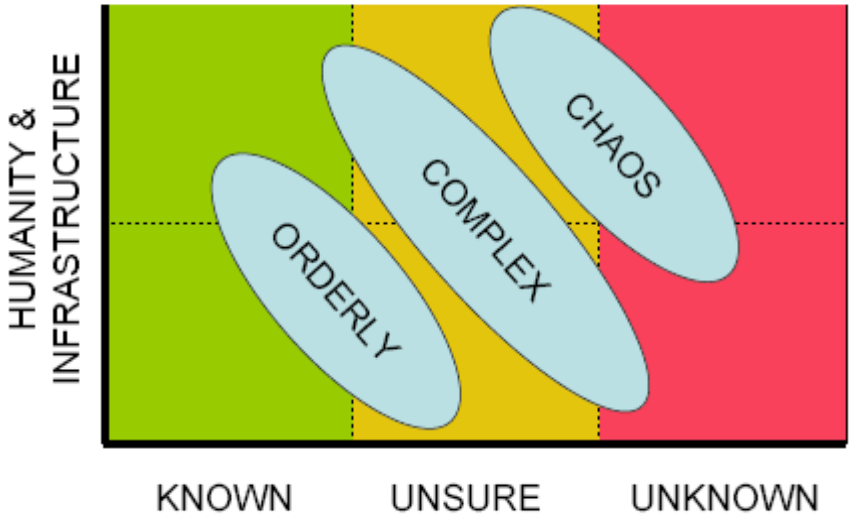

Figure 1. Characteristics of the Relationship between Cause and Effect in an HFN scenario

B. THE CONVERSATION SPACE IN HFN

Scenarios that stretch from a simple task of a fireman reacting to a local fire incident, to a response team reacting to civil unrest, to a major disaster like the Tsunami all require the implementation of an HFN. A successful HFN is one that can be quickly mobilized and deployed to facilitate an organized and coordinated response team using the conversation space as a place to plan and execute.

> The ongoing need to communicate and coordinate is fundamental for the success of the HFN. The term conversation space was introduced for the medium in which all this takes place – from forming community responses to delivering actions. The conversation space is (1) a medium of communication among (2) a set of players (3) who have agreed on a set of interaction rules. Peter J. Denning

Based on this, the HFN has to cater to the requirements of this conversation space, namely the collaboration infrastructure and the human organization structure. For the former, apart from advanced network technologies, research has also found that collaborative information technologies [1] has a key role to enhance the effectiveness of the HFN among the players. As for the latter, an adaptive organizational structuring system and framework is the way to strengthen the strategy.

C. IDENTIFIED GAPS AND ISSUES IN GOLDEN PHOENIX

Challenges faced in past HFN scenarios were studied before becoming part of the observation team's focus in Golden Phoenix. OGP was used to identify gaps and issues in our experiment preparation. These challenges serve as a focal point of our observation and a basis for reality in conducting the training or experiments.

Past Challenges vs OGP observation. The following paragraphs list the mapping of the observed gaps and issues in OGP in comparison to the past challenges identified in HFN scenarios.

1. Technology

a. Interoperability Between Communication Devices

Past Challenge: Each participating agency will operate on its own communication devices, and different agencies use different devices. Disparate radio communication systems do not interoperate easily. Provisioning of compatible radio sets must be done for organizations whose radio systems have security features enabled (e.g., encryption keys modulated with the signal for secure communications.) Typical military and emergency first-responder communication networks have such features.

OGP observation: The lead agencies, such as LACoS and LACoFD, have compatible radio devices riding on the same network. The MAG46 group was

provisioned with the same device by LACoS. However, during the social unrest "incident" at the Rose Bowl, when resources (assembled from all over the county) arrived, frequency allocation was not well managed. Frequencies were not coordinated among the response teams. Thus, teams were not able to communicate with each other - causing confusion for command and control on the ground. Another oversight was the capability of the system; when the response team moved into the basement level, the radio devices fell out of the "coverage area."

b. Differences in Communication Taxonomy

Past Challenge: Participants from multiple agencies, each with different backgrounds and standard operating procedures, congregate together to work hand-in-hand for a common goal. Typical issues include the misaligned taxonomies of information; classification, organization. Also, the ordering of information based on institutional procedures is different. For example, the military counterpart (operating in an "unknown" environment) used latitude and longitude to represent location, whereas the emergency services officers from fire, sheriff, or police use street names, buildings, and other landmarks for descriptions of locations (due to their familiarity with the environment.) Another example is the homeland emergency service team comprised of fire and police, which may have a different classification for an incident. For instance, it may need to be pre-determined whether a bomb explosion in a building should be classified as a fire or as a bomb explosion.

OGP observation: In this exercise, there are no significant problems as far as the taxonomy used in the activities. Each agency was well prepared, in advance, on the flow of scenarios. The training and information dissemination between agencies was also well understood and coordinated. Standardized taxonomy was in place; in particular, the military communicates its location in terms of street names and landmarks with the homeland emergency services team. However, the drawback was that most of the activities were made known in advance; they lacked the element of "surprise" that typically causes communication taxonomy confusion among the agencies. Unfortunately, the command and control system was not able to standardize or share information with other agencies, or at least among the lead agencies.

c. Supporting Infrastructure

Past Challenge: Availability of the infrastructure to support the deployment of technology equipment. For example, power is the most basic necessity for the continuity of operations for all technology equipment deployed. Thus, the issue of sustaining power and lighting for the operations area has to be considered. The challenge lies in the accessibility and availability of the necessary resources to provide electricity in the humanitarian response campsite or command center, not to mention extended needs for prolonged deployment that will cause more strain on all the equipment. For example, certain stretches of the low-lying areas in the Tsunami disaster are not accessible enough for deployment to even take place. In general, some potential DR environments will have poor access for food and fuel distribution.

OGP Observation: The on-site OGP experimentation lasted four days excluding preparation work. The Mobile Command Post (MCP) is a quick deployable "field" command center that provides space and connectivity to facilitate the information hub. MCP of various sizes were deployed in Los Alamitos Camp (the main operating site for OGP). Basically, the pack–and-go command post capability has improved tremendously with all the necessities becoming integrated. For instance computers, communication equipment, meeting rooms, and even a restroom are included. But, for DR operations to be successful across the board, the site has to be easily accessible by vehicles, which may or may not have "off road" capability. Most of the MCP deployed with ease to the simulated base camp and brought enough fuel capacity to support its own power generation throughout the exercise. Although some smaller types of command vehicles used internal fuel (shared the same gas tanks as the main engine of the vehicle) they were still self-sufficient because they usually had a more mobile mission that required them to move around from scene to scene. External fuel disruption was not simulated, thus refueling was easy. Communications networks in MCP were mostly facilitated by Wireless LAN and Satellite communications for long haul (or Internet) connectivity. The MCP contained the required command and control communications system that enabled collaboration between the first responders.

The military deployed a traditional command center complex made up of tents. A huge portable external generator was also deployed to support the command

centers in the military tents. Laptop computers, projectors, network equipment, and a Ground Antenna Transmit and Receive (GATR) satellite system were wired up. The main advantage of such a command center, compared to MCP, is the ease of deployment in rough terrain that is not accessible by vehicles. Thus, in comparison to the traditional command center, the Vehicle MCP will fare better in an urban environment.

d. Overwhelming Need for Resources

Past Challenge: Resource challenges are especially critical when the dynamics of a scenario are complex or chaotic. In short, resource demands are high and supplies are limited. In a typical scenario where casualties are mounting over time, every humanitarian mission commander would like to apply all available human resources in order to save as many lives as possible. For example, in the September 11 attack, all the fire and police officers immediately rushed to the site to save lives. On the other hand, in addition to human resources, material resources are also key (e.g., ambulances, police cars, fire engines, helicopters, and even portable generators.)

OGP observation: In this training, every agency was well equipped with technology resources, from MCP to satellite communications. Probably based on past experience from Katrina and the September 11 attack, agencies today are more ready to equip themselves with all the technology resources. In contrast, there were so many MCP deployed. In addition, each agency deployed its own satellite communications. About ten WIFI access points were made available at the unified command area. This raises the question about the need for consolidation of C2 and for efficiency optimization.

e. Interoperability Between IT Systems

The huge proliferation of ICT in recent years has led to each DR organization creating its own operational system. However, the interoperability requirement to connect systems from multiple agencies in an HFN scenario may not be well anticipated. Thus, interoperability interfaces are not planned for or built into the system. In another words, less interoperability between systems deters information sharing between systems.

OGP Observation: LAcoS and LAcoFD took steps to have a common command and control system. Compared to other agencies, these two lead agencies are able to share a common situation picture for awareness easily. However, the drawback was that external sharing was not incorporated. The MAG46 group deployed its own system on the Internet to achieve the sharing of information with them and other participants.

f. Dual Use Technology

The current peacetime system such as the radio communications network or public telecommunication network may not be capable of supporting a transition to an emergency mode. In short, there is 1) insufficient capacity to meet the overwhelming demands, and 2) survivability of these systems under the impact of a catastrophe is doubtful. The most glaring example from the September 11 attack was the overwhelming demand on the cellular communications networks. The first responders were unable to communicate with each other during the first few hours. Apart from all these problems, the advantage of dual-use technology to the first responders is the ease of transitioning from peacetime to an emergency situation with high readiness and efficiency.

OGP Observation: Most of the first responders in OGP rely heavily on their standard or personal cellular phone and service and their respective organization radios for voice communications. In a real disaster scenario, the availability of such normal service is questionable, especially if there is no power to operate the cell sites.

2. Organization

a. Lack of Coordination

When the roles and responsibilities in a scenario with multiple agencies are not clear, organizational coordination is weak due to the presence of multi-jurisdictional and organizational bias. The disparate agencies are typically unable to coordinate appropriately with each other.

A commonly known example is the conflict of organizational structure and culture between the civil and military components of a collaborative HA project.

OGP Observation: Civil-military coordination was not a major issue since this operation had as a major focal point the improvement of these types of operations. Apart from semantic information exchange problems encountered by both parties, the military was observed to have moved out from their typical C2 system to a much more collaborative platform (*Siteframe*; see annex OGP observation report for more details) in the Internet space.

b. Info Glut

Sometimes it is not the scarcity of information, but the glut of information facilitated by today's technologies that bombards and strains the command capacity.

OGP observation: The problem of information glut did not really occur since there was little system usage between participants because the system shared by LAcoS and LAcoFD was newly deployed. The MAG46 was using siteframe portal to collaborate with the civilian counterparts.

c. Adopting Hierarchical Command Model

Past scenarios show that typical hierarchical organizational models were directly flattened for HFN use. The traditional hierarchical organizational processes are not efficient when compared to the de-centralized organizational models because the hierarchical system will create an information gap in the HFN scenario.

OGP Observation: A unified command initiative was set up, which contained representatives from lead organizations to make command decisions. Formalized unified command briefings and discussions were held frequently. The unified command was a good initiative to flatten the various hierarchical structures, however there was very little meaningful activity occurring within the unified command. It seems that many of the activities are self-run. It may be due to the fact that, the work put in prior to the operation was so detailed that it enabled each organization to work on.

3. Sociology

a. Human Needs

According to Maslow's *Hierarchy of Needs*, the basic needs (such as shelter, water and safety) of the first responders must be met.

OGP Observation: Much of the MCP that were set up in the operation were well-equipped to provide the basic needs of the first responders. For example, there were restrooms and food storage/prep areas in some MCP. Even the operating condition of the MCP is made office-like in terms of look, equipment, temperature etc.

b. Emotional Volatility

Lack of information on a situation appears to be the main cause of emotional volatility. The command under this kind of situation will undergo cumulative stress that will eventually incapacitate the decision-making process.

OGP Observation: The list of activities and scenario developments were well documented for this exercise. Therefore, there were no signs of emotional volatility from the participants.

4. Environment Effects

a. Urban Area Effects

Mass casualty, congested operations areas, building instability, massive damage, and congested public communications are disastrous events for urban areas.

OGP Observation: Since OGP exercised the scenario of an earthquake in the heart of LA County (a metropolitan county,) it was a good initiative to simulate public unrest created by emotional impact. Exercises like this can go a long way toward preparing for a real-life DR event.

However, massive infrastructure damages that impede the current accessibility and deployment ability of a unified command asset were not exercised, especially with regard to the emergency response team voice communications assets.

b. Rural Area Effects

The typical traits of rural effect are a huge operation area with scattered population, poor deployment infrastructure in the way of transportation, power, communications, other necessities, and poor terrain knowledge. These kinds of environmental constraints pose a great challenge in HFN activities.

OGP Observation: The rural area effects were not a relevant scenario play since L.A County does not fall into this category.

D. NEEDS ANALYSIS

Observed data from OGP regarding activities between various organizations and the types of systems deployed profess the following purpose and attributes:

1. Creating Awareness of the Situation (intra-organization)

This is the fundamental need in accordance to the OODA (Observe, Orientate, Decide, Act) loop cycle concept that originated from Col. John Boyd, USAF. Each organization will equip itself with all the tools to understand the disaster. Information sources vary from watching broadcast news and reading reports to eye-witness observations from "ground zero." For this reason, positioning the relief team (or command) near the DR site is the best way to maintain situation awareness (SA.)

In OGP, each organization is well prepared with technological tools for SA. These technologies are communications devices such as cell phone, radio communication devices, satellite television, live broadcasting of video feeds, etc.

2. Sharing Awareness Among Organizations (inter-organization)

Each organization has its own resources to gather the required SA, and the domain knowledge of each organization will have its own cognitive appreciation of the disaster. The essence of details captured by each organization may be different. In the planning phase (evaluating or designing a solution as a unified team) — SA has to be shared and baselined, in order to achieve a coherent solution.

In OGP, the unified command, headed by LACoS, was formed to handle the disaster with other agencies well represented in the command structure. Meetings were held periodically throughout the operation to exercise the action plans, discuss suitable command structures that would keep everybody in sync and sharing situation awareness. However, due to significant prior preparation of the events and the widely distributed scenario, an element of "realism" was lacking. Agencies had little reason to coordinate due to the highly structured nature of the event.

3. Getting Different Expertise or Authorities to Work Together

HFN supporting actual DR operations typically face a much larger challenge than supporting normal military operations. The complexity of the disaster usually requires huge human resources and experts from various domains to work together and this is the biggest challenge to achieve efficient collaboration. The organizational participation grows proportionally with the area of operations and the severity of the disaster. The range of organizations with disaster relief expertise includes civil emergency response teams to fire, police, hospital, homeland security, and the military. Extended participation may include representatives from local, state, and federal governments, along with NGOs.

In order to handle the simulated catastrophic 8.0 magnitude earthquake, OGP simulated a wide range of organizations to provide assistance for the relief operation. The objectives were to train to work together (interoperate) effectively and efficiently, despite clashes of their inherited cultures, politics, or even technical systems.

4. Collaboration Environment

The set of tools and a platform to facilitate the collaboration of multiple organizations "to talk" in the HFN conversation space were discussed earlier. The purpose was to share information (to stay current and avoid information gaps,) manage resources (both in people and logistics,) develop and execute plans, and evaluate execution.

The environment consists of a platform and a set of basic tools that are easily accessible (despite the security considerations,) user friendly, reliable and efficient. [1]

"*Collaborative IT tools have the potential to transform the nature of collaborative group works,can create value by enhancing group performance.*" The findings reflect a similar hypothesis on the impact of collaborative IT tools in HFN that it can similarly enhance the performance in terms of effectiveness and efficiency.

What is the required list of collaborative IT tools and platforms? Particularly, from the collaborative IT tools perspective, in OGP's observation we have identified the Internet, shareable workspaces that enable information publishing and retrieving, video conferencing, Voice over Internet Protocol (VoIP), email, chat over instant messaging, and scheduling. The great dependency on these familiar IT tools is a translation from a typical office productivity suite that has evolved through the development of information technology. As for the platform, it is the communication medium or network that enables information exchange—mainly radio for voice communications and a data network. Technologically, the platform of the communication network must possess attributes that contribute to the ease of deployment, manageability, scalability, and survivability to render its usefulness in the dynamic characteristic of HFN operations.

In OGP, a huge array of technology solutions and collaborative IT tools and communication networks were deployed on the ground. The absentees were a shareable workspace and a communication network that matched up the attributes demanded in a real-life scenario. Again, this is due to the deployment of fairly new systems by leading agencies and "standardizing" the shareable workspace to allow substantial data transaction.

5. Command and Control on Resources

The requirement of a command and control system is to exert command and control over both human expertise and logistics. Due to the kind of complexity involved and the inevitable strain on available resources, there is a need for a system to monitor and manage. The need was institutionalized by the familiar use of the existing C2 systems in organizations. Apart from the connectivity to the resource (for monitoring) and the specific computations to aid the decisions that eventually constitute the actions plans, it also encompasses procedures and an administrative channel that are institutionalized by the organization. There is always a need to monitor and manage

resources; however, the idea of using of an existing C2 system from other organizations should be discouraged. The built-in procedures and administrative channels in the C2 system may not be relevant in the hastily-formed structure of organization in HFN, despite having another barrier to connecting up "external" organizations that limits interoperability.

The LACoS and LACoFD have common C2 system in OGP to exert (simulated) command and control capability over resources such as law enforcement officers, fire fighters, medical staff, fire engines, ambulances, etc.

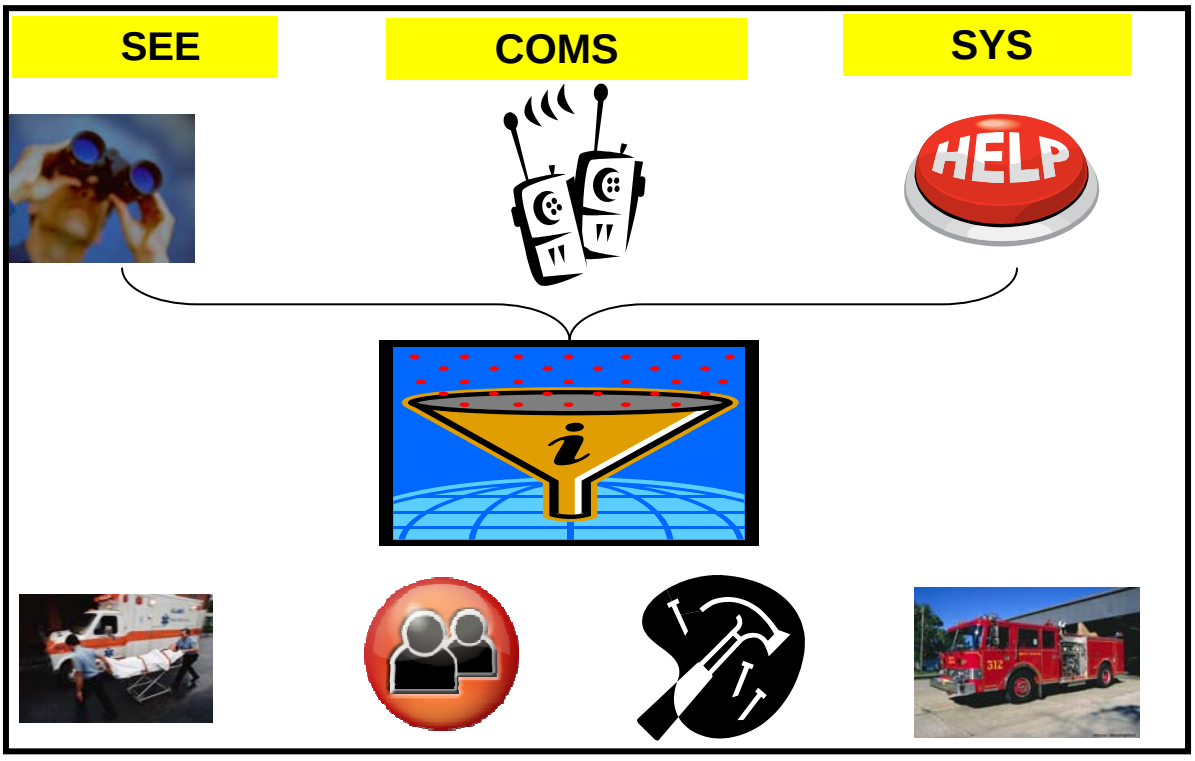

Figure 2. Needs Analysis for HFN

E. SUMMARY

This chapter examined the dynamics of an HFN scenario, in relation to the cause and effects, to provide an in-depth understanding of its nature and behaviors of the effects. The conversation space was identified as an essential piece that influenced its effectiveness and efficiency. Past scenarios developed together with observation from

OGP were analyzed and researched to provide an answer to where the typical problems or gaps occurred in the conversation space. The gaps are mainly subsumed into four categories: technology, sociology, organization, and environmental effects. Each category was the focal point of observation and discussion to allow needs analysis to be determined. The needs were further outlined and discussed to support the proposition for the integrated information system architecture analysis.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. INTEGRATED ARCHITECTURE

To design an integrated architecture that responds to the dynamic characteristics of an HFN scenario, we seek to achieve one common and unified system that will allow interoperability. That is, all functional components used by each organization will plug, play and share. The common info-architectural approach will lay the foundation to achieve a cohesive collaboration strategy amidst the multi-disciplinary problems. During the design, utmost consideration should be applied to the need for scalability, re-configuration, ease of deployment, and "plug and play."

A. IT SYSTEM

The architecture shall be based on knowledge-centric design since information demand is important in the multi-organizational aspect of the HFN. The effectiveness of the operation demands information sharing between functional groups. Thus, software systems must embrace an enterprise connectivity concept function as a service, autonomously allowing the system to interact with its service.

1. The Service-Oriented Architecture

Service-Oriented Architecture (SOA) is a multi-tier computing architecture that enables enterprises to share logic and data. It leverages the principle of a three-tiered architecture in the evolution of software engineering. In many aspects, the principle can be emulated in a multi-tier architecture. It is recommended for specific functions belonging to the individual functional group and it is typically shaped by the domain knowledge expert. Basically, SOA can be divided into three main layers, namely the presentation layer (i.e., Man-Machine Interface (MMI),) the domain/functional layer (i.e., business logic,) and the information services layer (i.e., data and information.)

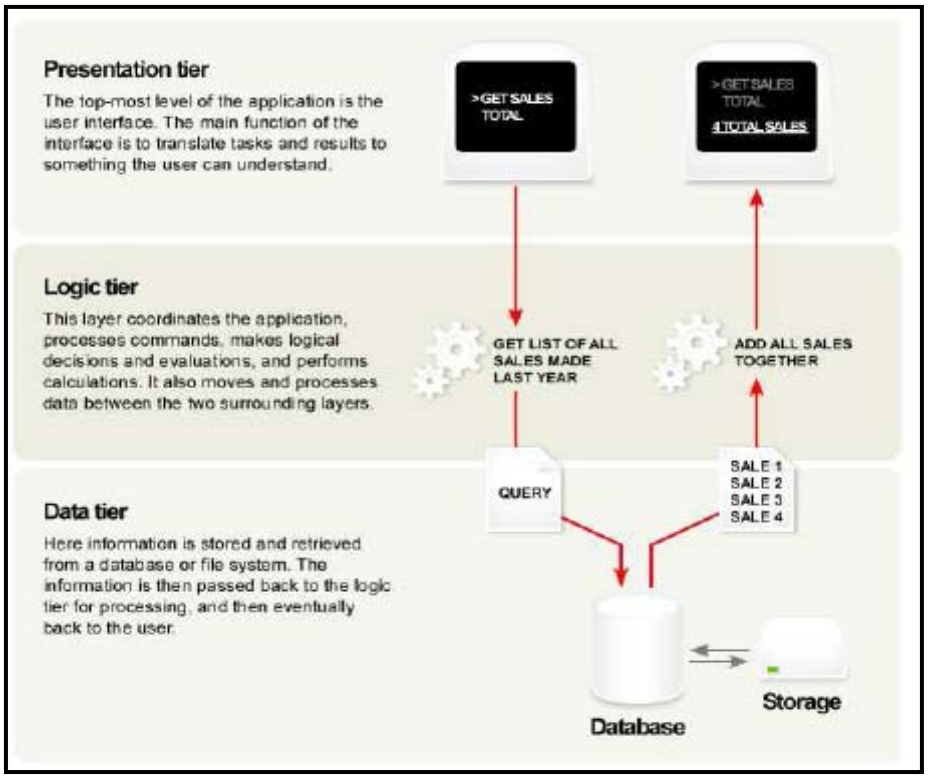

Figure 3. SOA Architecture [From 6]

a. Modular Design

By adopting SOA, transparency and autonomy are provided for in each layer. In short, clients' applications are isolated from the changes to the business logic and database structure. Scalability and security are more readily achievable through this model as the different tiers are not tightly coupled. The modular design will enable respective agencies to manipulate and present information effectively. Any changes in requirements can be accommodated with ease.

b. Knowledge Service

In a SOA, system behaviors are encapsulated by services, which are network-addressable components that can be used by another component based on a well-defined interface contract. It addresses the ease of interoperability with services dynamically discovered and subscribed to by the requester. Figure 2 shows a schematic on the service-oriented mechanism that can publish, discover, and subscribe. A more dynamic system is built with these loosely coupled components based on published

service contracts (interfaces, access protocols, and behaviors). Applicants need not know where the services are located. This location transparency characteristic is important for building scalable enterprise-wide distributed systems. The modular approach to development also enables new components to be added and existing ones to be modified easily. The dynamic nature brings us closer to the "plug-and-play" concept required. "System" and information become services that are easily defined and standardized for integral operations across a domain. On a higher tier, the focus will be on collaborative and decision support services.

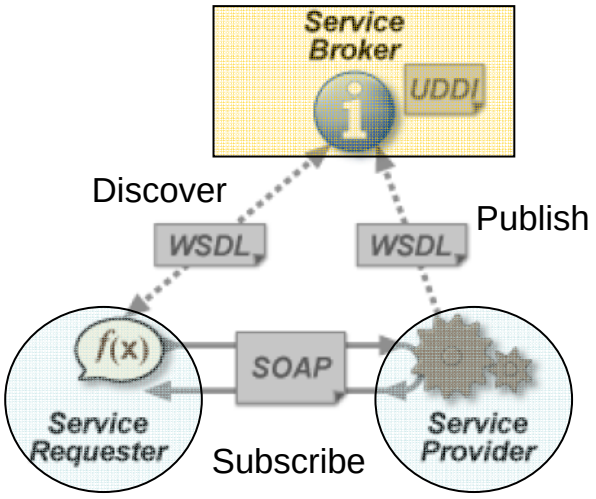

Figure 4. Schematic of SOA [From 6]

c. Synthesizing Systems

Each agency may have its own "stove-piped" or legacy system. A SOA makes integration/migration of legacy applications to the new Enterprise Architecture simpler. Lightweight wrappers can be implemented with new service-oriented interface/plug-ins to bridge legacy applications, further allowing their capabilities to remain available when the enterprise moves toward service-oriented architecture. Again, the modular architecture will allow front-end interfaces to remain unchanged, while migration plans can be put in place to gradually replace the legacy systems at the back-end.

d. Information Grid

The information grid dealt with the taxonomy of the domain information, interpretation, and presentation of data in accordance to domain. Simplistically, a police officer or fire fighter will want a latitude and longitude to be interpreted into addresses. Similarly, a soldier or a pilot may also need this service. The reverse is unacceptable. This is where the business/functional process layer has to perform domain interpretation logic.

2. The "Free-For-All" Portal

The complexity involved in the multi-organizational environment with uncertainty or unknown also called for the "Free-for-all" (FFA) workspace. This part of the architecture complements those functional capabilities that can be specifically built and discussed in the previous section. A web portal that is accessible by the Internet and uses WIKI's with a What You See Is What You Get (WYSIWYG) interface can be integrated with a host of collaboration tools (i.e., those that enable information publication and retrieval on a shared platform.)

3. SWOT Analysis

Albert Humprey's SWOT analysis technique is used to perform an assessment of the HFN architecture based on the Strengths, Weaknesses, Opportunities and Threats. Mainly, the SOA and "Free-For-All" system architecture will enable seamless knowledge-based collaboration (as a service) among the people in the HFN environment and its supporting communities (e.g., NGO, Homeland Defense, military, and coalition forces.) Also, the architecture enables ease of migration from a costly and complex domain-specific application to seamless enterprise-wide connectivity.

The table below depicts the analysis.

	INTERNAL	EXTERNAL
POSITIVE	**Strength** • Integrated System • Integrated Capabilities • Information flows with higher efficiency (reduce information gap) • Ease of system interoperability between agencies • Provide a collaboration platform	**Opportunities** • Groups collaboration will generate more ideas • Minimize indifference between agencies • Ability to handle mission more efficiently
NEGATIVE	**Weakness** • Single point system failure • Information overload since more agencies in the network • Network overload since so many agencies can link up • Conflicting opinions from "expertise"	**Threat** • Terrorism • No infrastructure to support electrical power

Table 2. SWOT Analysis Table on HFN Architecture

B. COMMUNICATION ARCHITECTURE

This section discusses the essential components required for the creation of an architecture that is suitable for the purposes of C2 as well as the coordination of various activities on an HFN. It is structured into the context of wireless communication using Wireless Fidelity (WiFi) and Worldwide Interoperability for Microwave Access (WiMAX) wireless technologies instead of radio frequency (RF) communication. The use of Very High Frequency (VHF) and Ultra High Frequency (UHF) radios, both military and commercial, are not considered due to the restrictions introduced by the radios, such as the constraints on operating range, requirement of locating the base station at a high elevation in order to provide line-of-sight (LOS) communication, and the small transmission pipe as a result of bandwidth-supportable RF communication.

The proposed architecture rides on the Internet Protocol (IP) based infrastructure. IP is a network layer protocol in the Internet protocol suite. It is a data-oriented protocol

used for data communication across a packet-switched network. It is encapsulated in the data link layer protocol. WiFi and WiMAX are examples of data link layer protocols. In this architecture, it is proposed that a dedicated intranetwork is designated "For Official Use Only (FOUO)" related applications and an "Unclassified (UC)" internetwork is designated for both FOUO and UC applications. Figure 5 depicts the architecture schematic diagram.

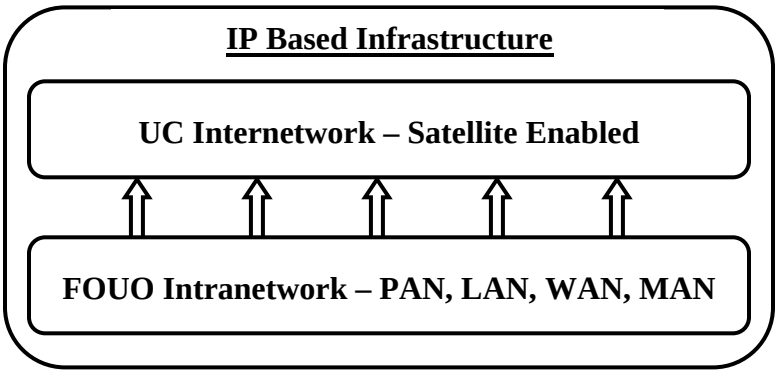

Figure 5. Proposed Communication Architecture

1. UC Internetwork

The UC Internetwork is connected to the public infrastructure via satellite communication equipment. Under no circumstances are users in the UC Internetwork allowed to access the information in the FOUO Intranetwork. In general, the public is the main group of users that will make use of this network for applications such as video-conferencing, emailing, and internet banking.

2. FOUO Intranet

The FOUO intranetwork is a dedicated network employed for the circulation of sensitive information such as command orders across the various usage segments (Personal Area Network (PAN), Local Area Network (LAN), Wide Area Network (WAN), or Metropolitan Area Network (MAN),) depending on the usage requirement. Information circulated within this layer is isolated from the UC Internetwork. Nevertheless, this architecture supports a one-direction access to the satellite-enabled internetwork for Internet-related applications.

3. Security and Sustainability

In an HFN scenario, multiple government and civilian organizations are deployed to provide humanitarian aid. However, the communication infrastructure is also required to support the general public. It is impossible to predict all vulnerabilities that are created by exposing this group of users to the network. In addition, the potential damage can be intentional or unintentional. This communication architecture supports the basic security and sustainability requirements for this type of multi-agency mission. Since the public is isolated within the Internet world, activities in the intranetwork can be performed securely.

C. SUMMARY

Following the analysis of the dynamic nature of the HFN scenario, we arrive at the discovery of the need for an info-architectural approach to be taken in the network design. Functional groups need to be able to offer their knowledge, expert analysis, and resources as services to other organizations. The benefits of a SOA with an FFA portal concept (that anchors the dynamism of collaborative needs) was discussed and proposed for a future information system development. Such a system would mainly host a suite of collaboration tools such as wiki, file sharing, IM, forum, PIM, etc.

The fundamental layer is facilitated by the communication platform — addressing both voice and data. Apart from the reliance on traditional radio communication infrastructure as the primary means of communications in a local disaster scenario, and assuming no disastrous impact on current radio infrastructure, a quickly-deployable network is necessary. The network architecture should accommodate the importance of having a secure and sustainable network structure and yet still be able to oversee the needs of the disaster-affected public.

THIS PAGE INTENTIONALLY LEFT BLANK

V. PROPOSED TECHNOLOGY IMPLEMENTATION

This chapter describes the implementation approach and the proposed technologies that meet part or most of the criteria discussed in the earlier chapters. (see Table 3.) Some assessment and evaluation of the availability of COTS products that are suitable and relevant to the proposed technologies are also recommended.

No.	Criteria Considered
A	**IT System (An SOA architecture)**
1.	Modular Design
2.	Knowledge Service
3.	Synthesizing Systems
4.	Information Grid
B.	**Communication System**
1.	UC internetwork
2.	FOUO intranet
3.	Security and sustainability

Table 3. Criteria Considered in HFN architecture

A. IMPLEMENTATION APPROACH

The empirical data collected from OGP clearly showed that massive numbers of people and organizations in the vertical domain are involved -- from local entities and state representatives to the federal level. Likewise, in the horizontal domain, the breadth of organizations involved ranges from emergency response teams and the military to NGO. From a technological viewpoint, developing and implementing a solution that touches the frontiers of all the organizations and people is not an easy task. The enterprise level implementation will involve political and sociological issues above and

beyond the technological choices. Achieving coherence among the multiple organizations will require multiple and extensive interactions over a long period of time. On the other hand, data from OGP observations also points to the idea of bridging the gap, making do with existing systems, and providing a basic collaboration space capable of achieving some effectiveness. (e.g. The implementation of siteframe portal by MAG46 command to provide a collaboration platform for civil and military) Though it is a rough road to take, with minor hiccups here and there, the task can still be accomplished. Thus, we propose a phased implementation approach with certain established priorities that is focus-based on the analysis of the previous sections.

1. The Steps

a. Identify Leading Agencies (decide what is available and re-use)

As discussed earlier, typical humanitarian relief missions are spearheaded by a few lead agencies. Usually, the military or the homeland defense agency's emergency response teams (e.g., the police, sheriff, and fire department,) have the lead over the multitude of responding agencies. Therefore, taking action and making improvements with regards to interoperability between these groups will significantly improve effectiveness and efficiency.

Taking a longer view, an enterprise level architecture design should be introduced within these organizations to improve interoperability and achieve a greater level of overall system efficiency. Adopting a SOA with the aid of a technology platform is the way ahead. However, the challenge of a design and development project of this scale is difficult to say the least – it requires moderation and synthesis of information across a spread of organizations. Therefore, a phased development approach must be mapped out, and the mapping process must start with identifying those services that each organization requires from the other.

b. Re-use of Existing C2 System

There are two main factors in the consideration of deploying the existing C2 system. If the disaster falls into a particular agency's jurisdiction, then the

management of their resources must be done through their C2 system. In this case, the idea of re-using the existing C2 is a viable and beneficial option. The immediate C2 of resources via existing connectivity with familiar systems is a huge benefit in terms of efficiency. Moreover, some of these systems have built-in computational algorithms to aid decision making or planning recommendations for resources. For instance, in OGP, LACoFD has a newly deployed C2 system that allows them to manage and track all fire engine resources. Checking availability and dispatching of these resources can be done through the new C2 system seamlessly and efficiently.

No.	Description	Deployment consideration remarks
Re-using existing C2 system		
1.	Area of operation located under responsibilities.	If the system has most of the disaster preparation template.
2.	Resources are manage by the C2 system	Possess extensive connectivity with existing resources, e.g., ambulance, fire engine, and police officers.
3.	Specialized decision tools embedded in existing C2 system	Ability to optimize and recommend resource to aid decision making.
4.	System security	System shareable with other organizations? If it is a concern, is multi-level-security architecture in place?
5.	Rigidity of system (when new procedure and structure of HFN is setup)	Ability to flatten its procedures and processes and adapt to new structures?

Table 4. Re-use existing system checklist

c. Work on the Collaborative Space (Set a Shareable Platform)

This requires a set of communication platforms and a web portal that enable information flow. Also required is a voice communication standard that enables first responders from different organizations to talk to each other through their voice devices.

d. Work on the Collaboration Tools (Give Them Tools to Work Together)

Identify tools that provide the following capabilities. They are:

(1) Web conferencing – supports point-to-point or multi-point low bandwidth web conferencing sessions.

(2) Instant Messaging – supports basic functionality of text communications exchange

(3) Integrated VoIP Services – supports voice and video conferencing over the IP network using computers or VoIP telephony.

(4) Collaborative workspaces – enable users to publish, manage and retrieve information of any file system from a shared workspace that is characterized by user groups, availability, knowledge, or skilled sets.

2. The Concept

The capabilities required by the organization can be divided into two groups: Strategic and Tactical. The strategic group is the unified command area where all the headquarters (HQ) or command elements of the lead and supporting agencies congregate. Typical setups will be more static in nature and exert overall C2 over the humanitarian mission with underlying communication linkages back to higher HQs and tactical groups. As for the tactical group, it will promote information collection on the ground with high mobility. Described below are the types of technologies or systems that are needed by each group to enhance SA and execute decisions.

a. Strategic Group

Key capabilities needed in this group are SA, incident/crisis management for tasking and events monitoring, collaborative workspace for publishing, and retrieving and sharing of information.

(1) WIKI Web Portal - WYSIWYG type of content management web portal that enables the users to publish, view, and share content on the web easily.

(2) Command and Control Application – A specialized system to manage resources and handle situations with known procedures and methods with similar operations undertaken by the agency's responsibilities. Although the system may be stove-piped and hard to interoperate, the benefit of having it to achieve immediate efficiency and effectiveness in the hastily formed situation lays in its immediate availability. This is especially relevant to some of the existing Decision Support Systems (DSS) from participating agencies that possess specialized analysis capabilities for the operations.

(3) Host of a Collaboration Workspace – A workspace that sits on an open platform is easily accessible to the whole community and supports the humanitarian mission. Preferably, this would be in the Internet environment, since this technology has rich connectivity to any part of the world. Furthermore, many supporting resources can also be made available through this technology. The workspace would enable users to publish, manage and retrieve information on any file system from a shared workspace that is characterized by user groups, availability, knowledge, or skill sets. The essence of the workspace is creating an avenue for information flow.

(4) Collaborative Tools – Basic functionality or tools to support the collaborative workspace.

Conference over Web – supports point-to-point or multi-point low bandwidth web conferencing sessions.

Instant Messaging (IM) – supports basic functionality of text communications exchanges.

Integrated VoIPl Services – supports voice and video conferencing over the IP network using computers or VoIP telephony.

Office productivity applications – since most of today's tasks revolve around email, word documents, spreadsheets, databases, etc., the availability of such tools is critical for enabling communication, publishing of information, and information flow.

(5) Connecting the Communication Platform – A set of COTS equipment, such as satellite communication equipment, WiFi APs, WiMAX APs, or wireless meshed devices that provide a persistent wireless connectivity across the AO. The use of multiple systems supports redundancy required in the operation.

(6) Managing the Communication Platform – There are three main criteria of a network management tool:

- Manageability – "Self heals" when the communication network expands and topologies become more complex.
- Security – Achieves "one to all" security policies across networks.
- Scalability – Supports new devices and applications.

b. Tactical Groups

The key capabilities that are needed include simple information alerts, reporting, and portable computing devices. Portability and mobility will be the focal points for ease of deployment. In the case of portable computing devices, we will examine the preferred choice of current technology (based on the survey conducted in OGP training,) devices that are similar to a hand-phone or personal digital assistant (PDA).

The "mini suite" of strategic systems – This is a requirement of all users (although the device has shrunk to the size of the cell phone and PDA.) However, the portal has been adapted to the characteristic of information display on a hand-phone or PDA.

Since the size of the screen is smaller, the display formatting and sizing and interacting styles (with regard to publishing) have to be specially handled to ensure quality human-computer interaction (HCI.)

(1) Information subscription and alerts – They are the eyes to "see" and hands to "feel" the unified command situation at the strategic level. The users at the tactical level are usually in a more precarious zone compared to their strategic counterparts. They require information subscriptions and alerts that provide the capability to be alerted immediately and reliably on situations that have an effect on their Functional Area of Responsibility.

(2) Simplified WYSIWYG web portal – The WYSIWYG type of content management web portal that enables users to publish, view and share content on the web easily is much more important here because of its small viewing space and limited maneuverability.

(3) Command and Control Application – A specialized system to facilitate the main C2 applications at the strategic level. It is usually a reporting mechanism with known procedures and methods similar to operations previously undertaken by the agency. Its purpose is to provide information to the main system at the strategic level that will facilitate situation awareness and resource management. Similar to the main system, it maybe stove-piped and hard to interoperate, but it is important to achieve immediate efficiency and effectiveness in the hastily formed situation. This is especially relevant to those systems that possess DSS capabilities that assist the tactical teams in their operations.

(4) Collaborative Tools - Basic functionality or tools to complement the strategic collaborative workspace.

Pod casting – supports pod casting sessions via a distributed network. The distributed broadcast will close the gap between every participant to enable a better near-real-time SA.

TwiddleNet – a distributed mobile server architecture that supports information-sharing through mobile web hosting.

Instant Messaging – supports basic functionality of text communications exchanges.

Integrated VoIP Services for live-casting – supports voice and video conferencing at the same time over the IP network using computers or VoIP telephony to facilitate the live casting of a situation.

Email application – mainly to facilitate an alternate avenue of flexible information flow from anywhere as long as the email addressee is known.

(5) Communication – A set of lightweight COTS gears, such as satellite communication equipment and WiFi APs that allow on-the-fly set ups and the ability to provide persistent connectivity. The systems must be mobile and robust enough to allow communication on-the-move.

	Strategic	**Tactical**
Characteristic	a. Unified command area where leading and supporting agencies congregate b. Huge numbers of people with lots of interaction c. Typically more static compared to tactical	a. Mobility b. Portability c. Mobile computing device – hand phone or PDA d. Small team operation
Software	a. WIKI Web Portal b. C2 Application c. Collaboration Workspace d. Collaborative Tools (web conference, IM, VoIP, office productivity suite)	a. Information subscription and alerts b. Simplified WYSIWYG web portal c. C2 Application d. Collaborative Tools (podcasting, TwiddleNet, IM, live casting, email)
Communication Technology	a. Satellite communication equipment b. WiFi APs c. WiMAX APs d. Wireless Meshed	a. Satellite communication equipment b. WiFi APs

Table 5. Technological Capabilities Needed in Strategic and Tactical Groups

3. Limitations

The technology recommendations proposed and discussed above are based on certain levels of technology similarities embraced by the people in their respective organization, especially the office productivity IT tools (e.g., MS Office.) The set of collaboration tools, network tools, and communications platforms mapped out from the needs analyses are fundamentally driven by their current usability, experience, and the perceived future of technology's evolution. Our proposed system will focus on ease of deployment and configuration to match various analyzed scenario.

The proposed technologies and architecture discussed so far are enablers for ameliorating cooperation and communication between a team consisting of participants from multiple organizations. Good practices that embrace effective and efficient collaboration are still necessary.

a. Convergence - Sharing a Common Goal to Achieve a Common Outcome

The command structure must synchronize efforts to unify the common goal of saving lives in the humanitarian mission. The environment is indeed challenging, given the participation from multiple organizations, various disciplines, cultures and domain knowledge, and the different preferences in the IT systems. Thus, to maximize the potential of the proposed technologies as an enabler, setting procedural standards and agreements in the use of the collaboration workspace and its tools is a good start. In a group-oriented IT platform, where information and content are open to manipulation by many, the usability is interdependent. One will feel frustrated and discouraged when information is inconsistently scattered everywhere.

b. Interdependency and Trust

For true collaboration to occur, fostering interdependency and trust is important. Recognizing differences in perspectives; a contradiction to putting in the "right" information, will strengthen the solution instead of conflict. To achieve effective collaboration, the trust between each pair of actors, whether between people or organizations, has to be there if there is any way to control the release of information or

to have privileged information management. The agreements and trusts have to be managed up front to avoid any doubtful intent or motivations.

c. Realizing Competency and Confidence

Over the years, people have formed certain intellectual beliefs and become comfortable using IT for collaboration or for completing their work. Great emotional preference is developed in procedural practices in their everyday domain. If there is a change in the tools used, a period of technology-familiarization will be required to make the users comfortable with the tools and to get their "buy-in" into the tools.

B. TECHNOLOGY RECOMMENDATION

This section evaluates the potential of COTS technologies and how these technologies can be integrated into the current systems of HFN to augment its performance during operations. The problems with the current system will be identified and proposed solutions will be discussed.

1. Collaboration Workspace & Tools – Strategic Group

Central Desktop is a good web-based collaboration tool that meets most of the demands required by the dynamic needs of HFN. Various types of features and technologies have been combined to provide an all-in-one collaboration workspace and web portal to facilitate a wide group of seemingly disparate users.

No.	Features required	Description of Features offered by Central Desktop
1.	WIKI Web Portal (WYSIWYG easy creation)	It supports easy creation of wiki web portals. Enables HFN users to upload and share info on web pages easily. Accesses right control for user groups and editing is provided. User gets to read "raw" information in html without sifting through tons of files, which is a good form of content management.
2	Workspaces (publish, share, retrieve files)	The workspaces that enable files to be published, shared and retrieved based on user group configurations. Supports all documentation and video management typical of office productivity suites. Updates on files are tracked.
3	Task management & monitoring	Provides a personal information management (PIM) that allows tasking and scheduling to be managed and monitored in a comprehensive portal.
4	Forum discussion	Encourages group discussions on a secured platform with customizable security policies and settings.
5	Web conference	Allows seamless integration to real-time web conferencing tools
6	Instant Messaging (IM)	Standard IM integrated to workspace
7	VoIP	Support VoIP application thru computing device

Table 6. Comparison of Central Desktop features to the required features

Items 6 and 7 are technologies that do not need to be integrated into the collaboration workspace. Typically, both web conferencing and VoIP capabilities need high bandwidth availability to produce acceptable levels of quality of service.

Therefore, it should be have a separate evaluation criteria for singling out a product with these purposes.

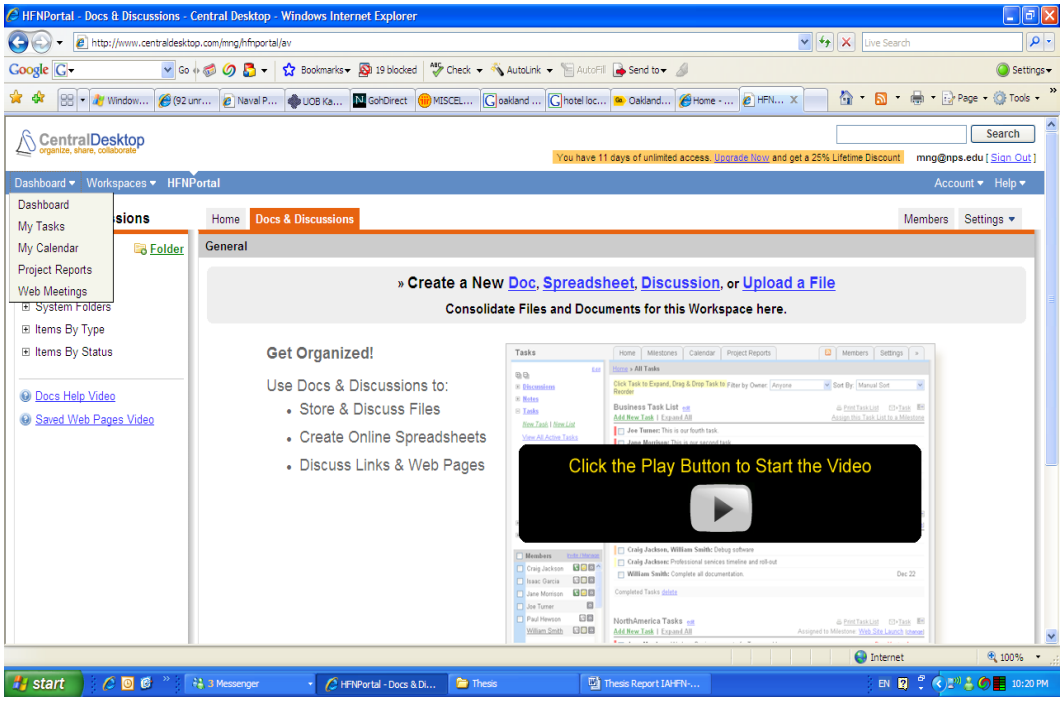

Figure 6. Central Desktop HFN "Wiki-like" Portal

The current limitation for Central Desktop is that the vendor hosts the application in the internet environment and the subscriber pays to use the service. For HFN purpose, it should be a comprehensive package that can be ported out and installed as an application on a server which is hosted in the unified command center to make it useful as a collaboration platform.

VSee is a good tool for performing web-conferencing and VoIP while using minimum bandwidth. It has the capability to adapt and tune itself to a network resource instead of using a hardware (e.g., Polycom) solution, while providing excellent web conferencing or VoIP quality. Such capability is critical since bandwidth limitations and contentions are problems often faced in the HFN.

2. Network Management Tools – Strategic Group [19]

In crisis management, different agencies from the federal, state and local government convene at the Unified Command Center (UCC) to coordinate the available resources for recovery missions. At OGP, we witnessed a typical setup of a UCC that involved a spectrum of supporting elements from NGO, military, police, fire, sheriff and

NPS Nemesis. To allow inter- and intra-connectivity, each supporting element was seen to be self-sufficient with its own satellite link to the public infrastructure. These links were extended via WiFi or WiMAX access points to reach their mobile entities. More than 10 wireless networks were detected at all times; half were secured while the other half were not. Such solutions allow seamless communications at the maximum bandwidth allowable by the satellite communication equipment. However, it is doubtful that all of the bandwidth was being optimized.

In conclusion, some form of network management tool is needed. These tools should have the flexibility to allow the integration of multiple access points, centralized automated enforcement of security policies, detection of unauthorized access points, efficient centralized management, and should allow automatic scaling when wireless networks are added.

a. Selection Checklist

A wireless network management system should enable network administrators to manage and troubleshoot the entire wireless network in the most effective and efficient approach. An example of a selection checklist is presented in Appendix B.

b. Management, Visualization and Detection – A Complete Package for HFN

Based on the operation requirements of HFN, Airwave Wireless Management Suite (AWMS) was selected. It introduces a robust solution that combines mission-critical requirements of management, visualization, and detection into a single console. The software is comprised of three components. The Airwave Management Platform (AMP) software used for configuration, monitoring and reporting, the VisualRF module for location tracking and RF mapping, and the Rogue AP Detection (RAPIDS) module used for automated unauthorized access-point detection. Depending on the operational requirement, AWMS is capable of managing 25 to 2500 wireless devices on a single console.

Figure 7. Airwave's Functional Capabilities [From 19]

(1) Airwave Management Platform

AMP is a centralized management system for the entire wireless infrastructure. It is a Linux-based application system that runs on standard PC server hardware. It is normally deployed in the network command center. The key features of the AMP software include:

- AMP supports real-time monitoring of all wireless users and devices on the network. It provides administrators with a holistic view from the network level down to the device level.
- The console allows controllers and wireless access points (WAP) to be centrally managed and thus allow efficient and homogenous proliferation of security policies throughout the entire network.
- Audit logs can be generated to contrast the current configuration of the WAP and controllers against the designated settings. Any discrepancies in the designated settings can be programmed to be corrected automatically by AMP as soon as they are detected.
- AMP is capable of supporting any mesh, WiFi and WiMAX hardware from a variety of vendors.

- Self-triggered fault reporting email or Simple Network Management Protocol (SNMP) traps can be generated by the software when a potential problem occurs in the network.
- Additional WLAN infrastructure to the network can be automatically detected by the software.

(2) VisualRF

VisualRF is the "eye" of AWMS. It provides administrators visibility to events that are taking place on the wireless network from the monitor window. It is able to provide mapping and as well as the location data of the users and devices in the wireless network through its software module. It uses sophisticated RF fingerprinting technology to accurately calculate the location of every wireless device in range and demonstrate its coverage pattern without having to deploy any sensor in the vicinity. The key features of VisualRF software are:

- It is capable of accurately calculating the location of each wireless user and device that resides in the network. Accuracy can be improved with more data points or carry-out surveys using the AirWave Management Client. Location of the devices can also be automatically recalculated even while on the move. This is achieved from real-time data feedback by the devices.
- By integrating Google Earth to the software, it provides administrators with a clearer representation of outdoor coverage and device locations.
- Strength of RF coverage in various locations can be represented on heatmaps.
- Interference and other potential problems are reduced by using color-coded channel maps.
- Amalgamated with AMP, the software is able to report errors when wireless devices fail or exceed their pre-defined thresholds.

- VisualRF is proficient in calibrating RF data from multiple vendors for accurate display in multi-vendor and multi-architecture environments.

(3) Rogue AP Detection (RAPIDS)

Having unknown or unauthorized WAP on the network can be destructive to the readiness of legitimate users in the wireless network. These devices may be installed by attackers to carry out certain forms of sabotage to the infrastructure. RAPIDS software offers the ability to detect 'rogue' APs on wireless networks. This module uses a unique combination of recovery methods such as SNMP and Hypertext Transmission Protocol (HTTP) scans to distinguish the different WAP on the network. The key features of RAPIDS software are:

- Wireless scanning using existing APs to detect and locate illicit devices within range of detection.
- Displays rogue device locations on the display window of VisualRF.
- Correlates information from wired and wireless scans and provides a score for each device in the network to indicate which may be likely to be a rogue device.
- Creates high-priority alerts that contain known information about the rogue device. The information can be the SSID, port number, security settings, IP address, etc.
- Shorten the time required to detect a rogue device instead of using a traditional wireless analyzer.
- Provide 'ignore AP' function that can prevent neighboring AP from being mistaken as an illegitimate AP.

c. Benefits to HFN

AWMS provides wireless management with a full range of operational and real-time monitoring capabilities. The software supports HFN operations in a number of ways.

(1) Visibility – In disaster recovery, the basic form of communication is through satellite communication links that have costly and limited bandwidths. It is of paramount importance that these resources are optimized and are used for legitimate purposes. AWMS is able to provide throughput information of the entire network without having to install specialized sensors or location appliances. All WAP in the network are closely monitored by the software. Information, such as the number of users, users ID, and the bandwidth usage of each user are represented in a graphic form for better appreciation of bandwidth usage. The signal strength and the Quality of Service (QoS) for voice versus data traffic can also be examined to allow simple diagnostics when network problems arise.

With more visibility over the wireless infrastructure, network administrators can specifically assign users to a particular WAP or reassign users to another WAP when a WAP is found to be overloaded with traffic. WAP that are less heavily utilized can also be relocated to other areas that are in need of them. Other than providing a platform for information sharing among the C2 and the supporting elements that are deployed to assist the recovery mission, the infrastructure is also provided to the general public for domestic purposes. With more control over the network, HA/DR planners will be able to segregate the networks into official and domestic channels without having to hinder the flow of information on the official channel.

(2) Flexibility – In missions with many participating agencies, it is predictable that equipment will come from multiple wireless technologies and architectures, including mesh networking, WiFi, and WiMAX. From what we have observed in OGP, wireless equipment that was deployed by various agencies came from different vendors. AWMS is able to support hardware from most leading wireless vendors to control the hardware from a single console and give a centralized operating picture of the entire wireless network.

(3) Security – In HFN, we are rather concerned about the type of network security measures that are installed into the wireless network. A HFN that is established to support a DR mission is a good intention, however, we cannot eliminate the possibility of criminals taking advantage of the already compromised situation by

attempting to get access to confidential information such as credit card details, internet banking login IDs, and passwords, etc., to reap monetary gain out of these data. However, it is almost impossible for the UCC to physically ensure that all devices in the wireless network implement stringent configuration settings that match security policies. To resolve the tedious work of physically configuring all the devices, AWMS provides HFN with a centrally-managed security feature. AWMS addresses this by performing automatic audits on the configuration settings of all devices within the network and compares the results with the security policies laid out by the network administrators. When a configuration error is detected, an alert with an audit log cites the differences between the actual configuration and the security policies. Depending on the severity of the error, different priority alerts can be configured for different networks. For example, errors in the official network can be a higher priority than those in the domestic network. AWMS can also be configured to automatically correct the errors as soon as they are detected.

Rogue WAP are possibly the next most common security threat. Attackers can connect to these WAP using their computers to sabotage the system. Similar to the operation of an Intrusion Detection System (IDS), AWMS is able to detect these illegitimate devices in the network and at the same time block their access to the network, enforcing the security policies within the network and saving valuable bandwidth.

From an information management perspective, we are concerned about the type of information that is being disseminated across the networks. Some high-level command decisions may be more sensitive than information on a routine change of duty, and general announcements that are broadcast across the network. The system administration of AWMS is based on a Role-Based Access Control (RBAC) mechanism. Each user of the network can be given unique login and access privileges depending on their responsibilities, which also restricts their access to only certain portions of the network.

(4) Manageability – In 2005, Hurricane Katrina caused severe destruction across the entire Mississippi coast and into Alabama, as far as 100 miles from the storm's center [20]. To extend communication coverage across the critical part of the

AO would have required an extensive set up of wireless technologies. It is almost impossible to carry out remote reconfigurations of wireless devices that are miles away from the network operating center. AWMS adopted a "push" methodology of reconfiguring the devices. A good configuration from an existing device can be efficiently and effectively pushed to a single device, a group of devices, or to all the devices in the network, reducing the management hassle and saving time for more important tasks.

(5) Usability – AWMS provides a simple human computer interface that allows administrators to navigate through the system and obtain a summary view of overall network performance that includes the number of up/down devices, and alerts on misconfigured devices. This information, when it is available at a glance, is time-saving in identifying problems in the network and for providing solutions to the problems.

(6) Scalability – The number of devices required in a network will vary depending on the coverage area. AWMS is available in various versions that can manage as few as 25 or less devices or up to 2500 devices with a single web-based console. This allows the wireless network to expand in a manageable manner.

3. TwiddleNet FLy Away Kit (FLAK) – Tactical Group

In emergencies and DR incidents, the levels of damage can vary in scale from day-to-day operations to large-scale and widespread catastrophic events. The levels of damage can be beyond expectation and preparation. In these scenarios, availability of ground information is critical. It provides authorities with the primary means of making hasty plans for search and rescue missions. However, we have seen in the events such as the September 11 attack, the Indian Ocean Tsunami, and Hurricane Katrina, that public networking and power utility infrastructures were completely destroyed and it takes days or weeks before these can be restored. Therefore, some form of on-the-fly communication network solution must be sought and proliferated down to the first responders on the ground to promulgate such mission-critical information.

a. Operational Capability of TwiddleNet

TwiddleNet harnesses the power of light weight mobile devices by providing a quick setup communication capability for first responders to enable them to react in HA/DR missions.

Using in-house developed software applications, TwiddleNet utilizes the built-in camera of mobile devices to provide instantaneous content capture and publish functions. As content producers, users can register their device profiles with TwiddleNet. As they capture content, it gets tagged and becomes available to TwiddleNet users instantly. While many of the tags are generated automatically, users have the option of providing additional tags for their content. Upon capturing of content, the owner has the liberty to categorize content before publishing it onto a mobile portal for more effective searching, or view and download it among users who have internet access. TwiddleNet portals work on a simple WLAN infrastructure. Their scalability allows them to be customized to the needs of the mission. They can be run on a handheld device to support a small first responder team, or on large computers to link together millions of cell phones sharing images, videos, and mobile-blogs. As users of TwiddleNet, people can search for content available on various personal mobile servers. Users can also register their interest in certain types of content and have an alert sent to them when that information becomes available.

This solution provides the first responders a complete and self-sufficient solution. First responders deployed to disaster-hit areas can conduct a ground damage assessment. Information on medical needs, water and food supply levels, images of wreckage areas, etc., can be delivered over TwiddleNet and circulated to participating HA/DR organizations for search and rescue mission planning. With better situation awareness and information superiority, appropriate equipment and resources can be mobilized for more effective mission recovery.

Other than first-responder missions, TwiddleNet is useful for a number of other applications including social networking, information sharing, and applications that require immediate content capture and dissemination, such as traffic condition reporting.

Key first responder requirements that TwiddleNet addresses are as follows [25]:

(1) Quick Set-Up. A key requirement of first responders, especially immediately after a disaster has struck, is to get going with their mission at the fastest speed possible. This means little time to set-up. The entire TwiddleNet system is designed to work with light-weight and battery-powered equipment. TwiddleNet fly-away kits, as explained later, include everything that the first responder team will need to get started with their mission.

(2) Tight-loop, Frequent Communication. An important task of first responders is to convey the ground reality to their co-workers and the control room. This needs to be done frequently and in real-time but without taking too much of the first responders' time and attention lest it start affecting their mission performance. To support this requirement, TwiddleNet-enabled smartphones produce tagged, xml-based, Atom feeds automatically on content capture. The entire process of generating and attaching tags to content is automated. Once content has been captured and tagged, the content is pushed automatically to those who need it and notices are disseminated to others so they can pull the content if desired.

(3) Light-Weight Equipment. Mobility is often an integral part of the first responders work. As a result, their equipment must be as light as possible. TwiddleNet uses smartphones, which are light-weight and small, but still provide the redundancy that is so critical to the mission success. In addition, the TwiddleNet portal itself can be run on handheld devices (PDAs or small handheld computers) to further reduce the weight that the first responder team needs to carry.

(4) Scale-up as Team/Requirements Grow. TwiddleNet is focused on the first 48-72 hours after a disaster, when the team size is small. As the situation evolves and the team size grows, TwiddleNet can hand-off to a more robust infrastructure (powerful servers) when it becomes available.

(5) Power. Due to their short charge life and weight, batteries that power the smartphones are an important concern. Often first responders have to carry spare batteries, which increase the weight they have to carry. To address this issue, TwiddleNet pays special attention to power management - it supports smart caching of

popular content provided owner consents. It allows the first responder to offload some of its serving functions to the TwiddleNet portal. In addition, to further conserve power, TwiddleNet supports several user-selectable content dissemination schemes.

b. System Requirements

TwiddleNet employs wireless technologies to provide interoperability between its clients. The basic components that are required to support this capability are:

Power. In remote deployment, providing power for the equipment used is the main concern. Examples of commonly deployed solutions are: lithium batteries that come with the equipment, solar power, generators, and even power from buildings, subject to the availability of the infrastructure. Modern gasoline generators are produced by many companies and offer very efficient power solutions for on-the-fly deployment. Honda's family of super-quiet inverter generators is one of those gasoline powered generators that are capable of providing such capabilities. Its inverter technology makes this generator ideally suited for use with sensitive electronics because the solution provides clean energy that prevents surging. Its light weight and easy setup features make this generator ideal to provide first responders mobility and ease of quick deployment. Its Oil Alert safety feature prevents the generator from any damage by shutting down the unit when gasoline drops below a safe operating level. This family of generators provides various rated powers. Depending on the power requirements of the system, the generators are available from 1000 to 3000 watt rated power. Table 6 shows the performance of this family of generators.

Figure 8. EU 1000I, EU 2000I and EU 3000IS

Model	EU 1000I	EU 2000I	EU 3000IS
Dry Weight	29 lbs	46.3 lbs	134 lbs
Dimension (L x W x H)	17.7" x 9.4" x 15.0"	20.1" x 11.4" x 16.7"	25.8" x 18.9" x 22.4"
AC Output	120V 1000W max. (8.3A) 900W rated (7.5A)	120V 2000W max. (16.7A) 1600W rated (13.3A)	120V 3000W max.(25A) 2800W rated (23.3A)
DC Output	12V, 96W (8A)	12V, 96W (8A)	12V, 144W (12A)
Run Time per Tankful	3.8 hrs. @ rated load, 8.3 hrs. @ 1/4 load	4hrs. @ rated load, 15 hrs. @ 1/4 load	7.2 hrs. @ rated load, 20 hrs. @ 1/4 load
Fuel Tank Capacity	0.6 gal.	1.1 gal.	3.4 gals.

Table 7. Honda Super Quiet Inverter Generator Comparisons

Portable Broadband Satellite Terminal and WLAN AP. With no other network infrastructure available, a satellite link is deemed the most practical and quickly deployable technology to provide a rear link to the public infrastructure for communication. Hughes 9201 Broadband Satellite IP Terminal with Wireless LAN Access Point, which interfaces over the Inmarsat BGAN satellite network, has many advantages that make it an attractive solution.

(1) Global Coverage

BGAN delivers seamless network coverage across most of the world's land mass. With this coverage, DR mission planning will not be restricted to specific areas. First responders will be able acquire their broadband access from any part of the globe.

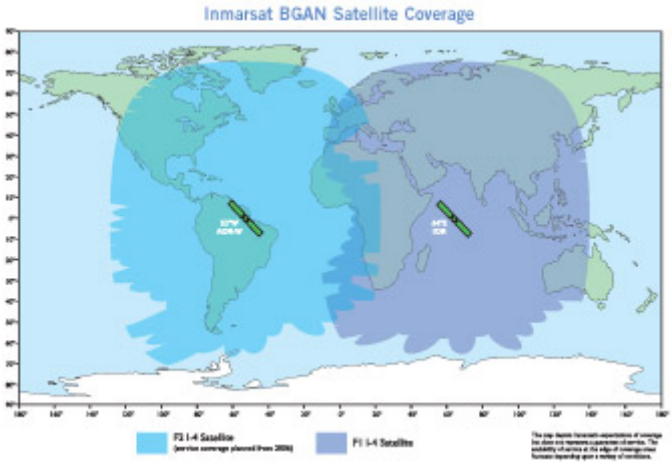

Figure 9. Inmarsat BGAN Satellite Coverage

(2) Easy to Use in Semi-fixed and Portable Environments

Hughes 9201 is designed for simplicity and ease of use. It is designed to be lightweight and compact to improve its mobility in deployment. Its IP55 ingress protection feature allows the terminal to be installed outside in harsh weather conditions for extended periods of time and in higher altitudes if required to overcome LOS communication issues.

(3) Simultaneous Voice and Broadband Data

Hughes 9201 is a gateway to global communications. It allows simultaneous send-and-receive IP packets and circuit-switched data via USB, Ethernet, ISDN, and WLAN interfaces over the Inmarsat BGAN satellite network. Its built-in WAP feature provides another avenue for coverage extension by integrating with another wireless networking device.

The Inmarsat BGAN satellite service provides subscribers with the convenient to access the Internet on-demand. However, due to the fact that it is a very niche technology in the communication field with not many service providers, the service can cost as much as $7 for a megabyte of data, which makes deployment of this technology very expensive. The cost factor should be considered during operation planning.

WiMAX – The Last Mile Technology. WiMAX (Worldwide Interoperability for Microwave Access) is the IEEE 802.16 standards-based wireless technology that targets providing wireless data communication over longer distances. So far, WiMAX can offer a solution to what is normally called the "last-mile" solution by connecting individual home and business office communications. This solution is more cost-effective compared to conventional communication technology as it does not require a physical data transportation infrastructure, such as an optics cable, to be available from the service provider to every individual household or office.

The Expedience® Compact Outdoor Subscriber Unit (OSU) is Motorola's first Non-line of sight (NLOS) product for the broadband wireless market. OSU is an environmentally-hardened broadband wireless solution that supports operations in extreme conditions. It is designed to be compact and flexible for fast installation. It is weatherproof and pole-mountable. It is capable of providing wireless coverage to an extended range of up to 32km. No software is required to be loaded on a subscriber's mobile device. Therefore, users can simply plug and play onto TwiddleNet. As WiMAX is still an emerging technology, there has yet to be any proven WiMAX clients on the market that are capable of supporting a direct link to a WiMAX access point. The compatibility issue between WiMAX access points and the client, (e.g., the connectivity between the Motorola Expedience OSU and the Samsung SPH-9000 WiMAX-enabled phone,) has yet to be addressed by any official WiMAX governing body. To overcome this challenge, the available solution is to employ a WiMAX to WiFi gateway for WiFi clients to be connected to the WiMAX cloud. However, this increases the complexity of wireless connectivity due to the requirement of additional hardware.

Mobile Devices. TwiddleNet exploits the power of modern mobile computing technologies by providing information sharing services among first responders and HA/DR planners. This on-the-move capability is viable, and uses WiFi/2.5 or 3G-enabled clients connected to the wireless network. .

There are varieties of mobile devices such as smart phones, PDA, PDA/mobile phone combinations, personal communicators, Ultra-Mobile PCs, etc., which have features such as the capability of providing mobility, increasing storage capacity, high resolution displays, improved computation power, keypads, and yet have low power consumption.

This allows these mobile devices to handle more complex applications that could only have been undertaken by conventional high- end laptops or desktops in the past.

Figure 10. Samsung SPH-9000 WiMAX Enabled Phone (Left) and HP iPAQ hw6945 WiFi Enabled Mobile Messenger (Right)

c. Deployment Configurations

The concept of TwiddleNet FLAK is a self-sufficient solution with a private wireless network infrastructure, with a power source to support its own equipment that can deploy in remote areas with no other resource means. Two deployment configurations are proposed.

(1) On-the-Fly. The On-the-Fly configuration is most suitable for deployment at times when a disaster has struck. At such times, there are no public infrastructures available to support any communication channels for information dissemination. In such a scenario, TwiddleNet uses Hughes 9201 and WiFi-enabled mobile devices. Hughes 9201 interfaces with the Inmarsat BGAN satellite network to establish a rear link to the public infrastructure. Once registered with a service provider,

mobile devices can be connected to the Internet via the wireless LAN connection for direct information sharing among the TwiddleNet users on their WiFi-enabled mobile devices. If extended operation is required, gasoline generators can be utilized to provide the necessary power.

(2) Operation-in-Depth. This configuration provides extended range coverage solutions for first responders operating deep in the Area of Operations (AO.) It has the capability to operate on available WiMAX links, or alternatively, it is self-sufficient with its own wireless equipment and can provide its own wireless link. This configuration is equipped with Hughes 9201, two Honda gasoline powered generators, Motorola OSUs, and mobile devices. Motorola OSUs, powered by Honda generators, will be collocated with Hughes 9201s to provide extended wireless coverage of up to 32km. First responders will be connected to the wireless link via their WiMAX-enabled client. Table 7 shows the comparisons between the two configurations.

	On-the-Fly	**Operation-in-Depth**
Equipment Required	- 1 x Hughes 9201 - WiFi enabled clients	- 1 x Honda generators - 1 x Hughes 9201 - 1 x Motorola OSU - WiMAX enabled clients
Set up	Quick and easy	Extensive
Link Established	WiFi	WiMAX
Operation Range	Up to 100m	Up to 32km
Operation Duration	Option 1: 36 hours on standby, 162 megabytes transmit or 864 megabytes receive subjected to wide range of factors and actual usage Option 2: 32 – 80 hours continuous depending on generators used.	32–80 hours continuous depending on generators used.

Table 8. Configuration Comparison

d. Concept Evaluation Methodologies

In OGP, a successful trial of the alpha implementation of the TwiddleNet concept was conducted by the NPS data collection team. The NPS data collection team carried out a trial of the ***On-the-Fly*** concept using Winodws Mobile 5.0 Smartphones equipped with camera features and back-end portal servers to facilitate the sharing of critical information within the area of operation via WiFi links connected through satellite communication systems. A feasibility study of the concept was carried out with key assessments on the operational concept, human factor analysis, and technical feasibility. A questionnaire survey was also conducted with the training troops. This report is based on our observations and the questionnaire survey with the users of our system.

(1) Scope of Trial. The objective was to study the operational and technical feasibility of deploying TwiddleNet to support first responders' collaboration activities, such as task-oriented work and situation awareness in an incident. The scope will cover:

- Deployment of TwiddleNet for technical assessment
- Collaboration tool concept testing
- Survey Questionnaire

(2) Preparation for Trial. The preparation of the trial was divided into two different phases. They are:

Phase 1: Identifying trial participants. The trial involves using the latest WiFi-enabled Windows Mobile Smartphones. To ensure that the trial was not influenced by the technicak competency of the users, candidates for the trial were carefully selected.

Phase 2: Preparing the participants. A short introduction of the concept and equipment training was given to the participants. Efforts were made to ensure that the participants were comfortable with the equipment prior to the commencement of the trial.

e. Findings

(1) System Setup and Deployment.

Ease of deployment. The required platform for connectivity between the devices is regardless of the type of data-communication technology. As long as it is communicating in IP protocol, the application on the mobile devices will work. In this training, the deployment was easy since most of the agencies use WiFi with connectivity to the Internet. Overall, the deployment was instantaneous in such an environment (with or without a WEP key imposed for security).

Multiple wireless networks. At the training ground, there were multiple WiFi networks being setup — about 10 networks. Most of them did not employ any Wired Equivalent Privacy (WEP) or WiFi Protected Access (WPA) security. Technically, with so many WiFis operating in the Industrial, Scientific and Medical (ISM) band and with no coherent management of the ISM frequency channel, the throughput of the WiFi was negatively affected. Operationally, this is confusing for the ground personnel and it did have negative effects on real achievable throughput.

Mobile device configuration. Each device has to be pre-configured with an identity for ease of identification and the information (IP address) of the webserver for reach-back purposes. The latter configuration is needed because the metadata of all posting is stored on the webserver, which is hosted on the Internet network. Current limitations on this webserver deployment are because the PDA's webserver packages were not ready to be deployed in time for the training.

Dynamic Host Configuration Protocol (DHCP). During the trial, we noticed that the users were unable to retrieve past data whenever the wireless network re-issued IP addresses that were different from previous ones. The current design of tagging the IP address of the device to the metadata, instead of the user name in the retrieving process, has caused this limitation. This scenario also arises when the users move into a different wireless network.

Software application for collaboration. The application stability is another problem that was encountered during the trial. On a few occasions, the applications needed to be restarted to restore them to a workable stage. This was especially true in the transition process, which was involved in taking pictures and

transmitting them, which was not smooth. Delays in data transmission were often experienced. Certain means of data compression techniques and data streaming techniques are needed to expedite the transmissions or recover from transmission failures.

Bandwidth competition. We have also observed that Internet connectivity was provided by satellite communications. Most of the satellite dishes mounted on vehicles do not provide enough bandwidth. Therefore, the bandwidth may be congested by multiple devices competing for the same resources. That is one of the probable reasons for frequent delays in transmission.

(2) Human Factors

PDA form-factor and features. During the conduct of the trial, the issue of handling of the Windows Mobile was repeatedly brought up. While the troops are operating in full gear, and some with gloves on, the styli and buttons on the keypads of their pocket PCs seem miniature. Some went on to highlight the requirement for an anti-glare screen so that the effect of temporary blindness, caused by the light emitted from the device, would not compromise their night mission.

Collaboration application. On software applications, usage should be limited to just a few clicks and a drop-down list rather than extensive entering of data or maneuvering. If possible, application designs should have buttons and arrows large enough to be pressed by a finger instead of a stylus.

Power sustainability. Some were also skeptical about the sustainability of the battery during real operations. It was recorded that extensive transmitting and receiving of PDAs can only sustain up to an estimated 7 hours. Backup plans such as a hot-swappable battery could be adopted to solve this issue.

Acceptability of mobile devices. Another concern that was brought out was the issue of HCI. The IT age has brought about a revolution of attention to stay technologically savvy. In this instance, ease of use is not a concern for those who are familiar with the know-how of simple electronic devices such as a PDA. Nevertheless, we could not ignore the fact that there is still a minority group that has scarce or no exposure to such electronics, and have problems accepting a PDA as a collaboration tool.

Therefore, software designers have to tailor their applications to a more user-friendly mode to cater to the needs of this minority group.

(3) Surveys

Deployment Concept. The interviewees were pretty impressed with the light-weight concept, especially as the eventual concept of TwiddleNet does not require any backend server or Internet connectivity. All data is hosted from the PDA itself as long as the network connectivity is achievable on the local site. There is nothing much to setup since configuration is minimal. But, most of them are unaware of the complication of the network and hardware involved for other alternate systems that have a backend as the hosting server.

Perceived Usage at Command level. Most of the interviewees felt that such mobile devices were more suitable for personnel at the command quarters rather than personnel that are hot on the scene. There were "not enough hands" to use a PDA for information; voice communications are a better preference in the latter scenario.

Instantaneous Situational Awareness capability. The survey found that the software application has provided first responders a simple platform for the easy sharing of information in the form of pictures or text. Some even commented that they have the freedom to post information collected without much consideration since it is hosting from its "personal" webserver. With these, more information will be freely available and made sharing more easily. However, information overflow may also be a problem. Thus, certain monitoring mechanism, such as a subscription log should be incorporated to provide user with an update of the memory status.

An effective way to have information on hand. Most users are in favor of using a PDA for information updates and SA purposes without the hassle of sitting in front of the computer terminal and looking at the thing. But some of them are still skeptical about its power compared to a desktop computer for serious accomplishments.

f. Trial Conclusion

So far, we have discussed some of the glitches observed during the trial. From some analyses and discussions with the participants, we deemed these problems solvable technically and through proper standard operating procedures. The participants were in favor of the operating concept due to its mobility and its capability to disseminate information in real time in a first responder environment. This concept also complements their existing network-centric equipment. However, familiarizing users with this equipment is of paramount importance. The requirement of a dedicated WiFi network via a satellite link is necessary to maximize the potential of this concept.

g. Operation Considerations

The two solutions offer first responders' access to the Internet at times of critical need, however, there are some considerations for the two solutions.

The WiFi-driven solution is limited by the nature of WiFi networks' operating ranges. A typical WiFi network using 802.11b or 802.11g standards might have an operating range of 100-300m outdoors. Although directional antennae can be used to boost the coverage, additional hardware will have to be set up. Consequently, users will be limited to operating within the signal-detectable range. Nevertheless, this drawback is compensated by its mobility and simple setup procedures.

Weighing only 2.8kg, the Hughes 9201 provides first responders the ability to deploy the system conveniently to meet their operational needs. To establish the wireless connection, BGAN application software is executed from a laptop computer. Using Global Positioning System (GPS), the software identifies the location of the equipment, and provides the antenna angle and the recommended compass direction that the antenna should be aligned to. When a satellite signal is detected, hardware can then initiate registration with the service provider. The average setup time is about 10 minutes. This simple setup procedure allows first responders to utilize TwiddleNet services hastily. With the advancement in WiFi technology, COTS WiFi-enabled mobile devices are widely available on the market. Issues with regard to QOS, bandwidth allocation, and other technical problems have been taken care of ergonomically.

WiMAX operated solutions provide a new set of benefits and challenges. WiMAX networks provide coverage without sacrificing bandwidth. Its grant-request access protocol does not allow data collision and therefore uses the available bandwidth more efficiently and is capable of delivering broadband speeds to end-users throughout a cell to ranges of up to 32km. Extensive setup processes are required to deploy Motorola OSU on high ground for wider range coverage. Depending on the type of power source used, this solution is able to provide wireless communication for up to 80 hours. The scalability feature provided by Motorola OSU also allows multiple TwiddleNet users to operate currently within the AO.

Unlike WiFi technology, WiMAX technology is still evolving; the most significant challenges are technical support and the availability of COTS clients. At this time, there are minimal WiMAX-enabled mobile devices on the market, such as the Samsung SPH-9000. Mobile device giants such as Motorola have just announced their success in designing and developing a new WiMAX chipset, which will be incorporated into the next generation mobile devices starting in 2008. Despite the development, the compatibility issues between WiMAX access points and clients remain unclear. Until the evolution of WiMAX technology is complete, its reliability will still be questionable at times of critical need.

4. Extending the Coverage – Tactical Group

The coverage of wireless networks such as WiFi and WiMAX can be limited by a few factors such as the performance of the hardware and environmental factors. To deploy multiple base stations to provide extended coverage can be impractical in a disaster-hit area. In this part of the thesis, a re-broadcasting solution will be proposed. It is best suited for non-hostile applications such as DR, surveillance and protection, or special events. This simple solution uses the concept of a helium-filled balloon to provide the "lift" mechanism for communication equipment that acts as the re-broadcasting station for data transmission beyond the range of a hop. This solution provides first responders with a simple and mobile way of extending the distance coverage for users that are far away from the main Internet cloud.

a. Balloon-Based Communication Nodes

Balloon-based communication nodes customize commercial-use platform and COTS communication equipment into one solution to meet the most stringent requirements. The pictorial representation of the solution is presented in Figure 9. Helium balloons and airships are widely used in commercial applications. In order to provide the "lift" required for these platforms, helium gas is often used. Helium gas has the properties of low boiling point, low density (lower than air), low solubility, high thermal conductivity, plus it is inexpensive. These characteristics make it attractive for providing a safe and low-cost solution for providing the lift for these solutions. Depending on the type of communication needed in the operation, the payload can be customized to wireless mesh, WiFi and WiMAX, Mobile Ad-hoc Network (MANET), Repeater/Rebrocast (REBRO), military radios, monitoring and surveillance, or a combination of these. Lightweight high gain omni-directional antennas can also be included as part of the payload to increase the overall performance. The holding fixture of the solution includes an anchoring ring that holds the balloon and the payload. A ring is chosen to provide more balance. The communication line connects the payload to the ground module where the Alternating Current (AC) and Direct Current (DC) power sources are located.

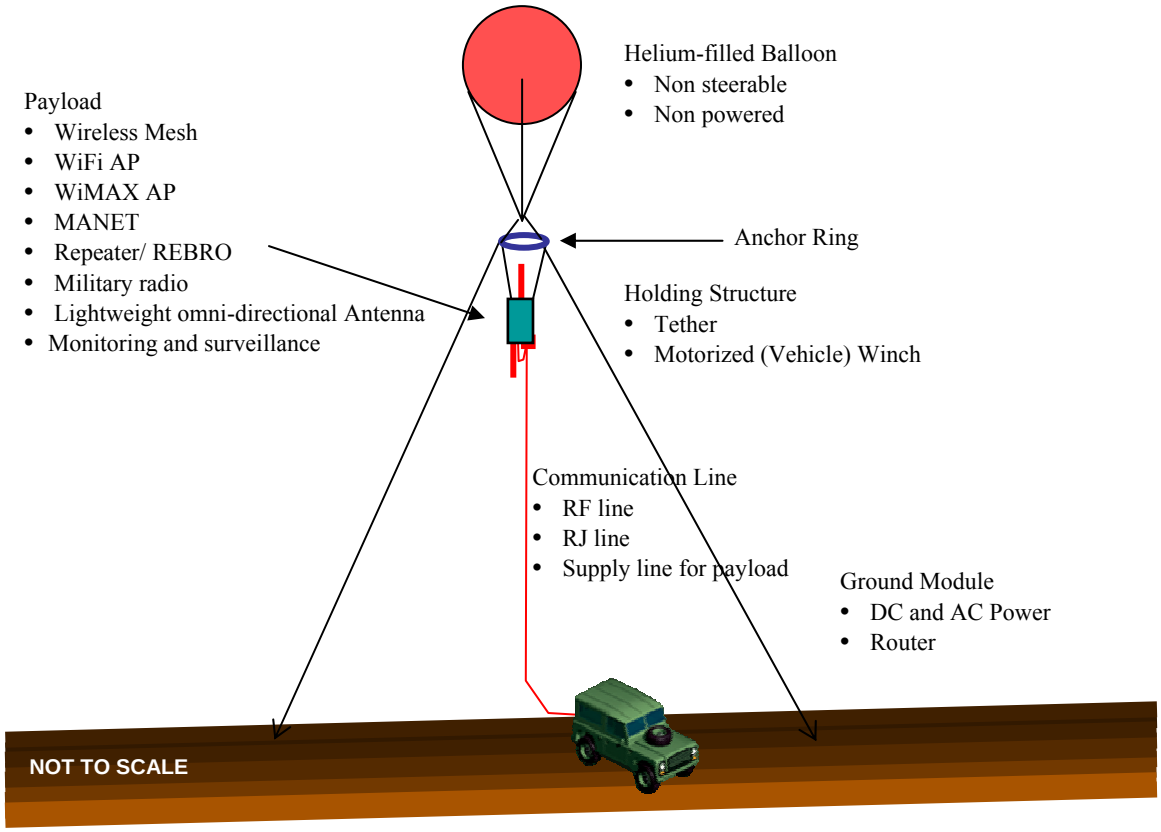

Figure 11. Balloon-Based Communication Node (From Singapore Technologies Engineering)

b. Benefits to HFN

Building tall base stations in an emergency scenario to house communication equipment for wireless network coverage seems impossible. A balloon-based communication node provides HFN with an alternative that allows a mobile and quickly deployable solution. Depending on operation needs, payloads can be configured instantaneously with a variety of gears to support multiple functions. The operation of this solution can be affected by the environment factors. In case of adverse weather condition such as a strong wind and thunder storms, it will make the solution almost impractical.

c. Design Considerations

As this is a customized solution with a possible alteration in payload, the designer must take into consideration various factors such as the weight of the intended payload, the operation environment, and the local authority restriction on the height of balloon deployment.

C. SUMMARY

This chapter discusses both strategic and tactical solutions that are capable of augmenting the performance of HA/DR missions. The strategic group addresses the technologies needed to achieve SA, incident/crisis management for tasking and events monitoring, collaborative workspace for publishing, and retrieving and sharing of information. The tactical group describes some on-the-fly solutions that were customized from simple mobile devices that are capable of providing information alerts, reporting and sharing via smartphones as well as systems-of-systems technologies that are capable of extending the coverage of WLAN communication. The systems recommended are customized from COTS and addressed the current limitations of HFN.

VI. CONCLUSION

A. CONCLUSION

The results of the study done on past HFN scenarios, together with the analysis of observation data collected in OGP, have brought up a number of interoperability issues between organizations. These issues remain unresolved and continue to be challenging despite experience in a number of recent HADR missions. The dynamic nature of the communications requirements encountered in HADR missions require the HFNs to be architected such that the various agencies can to collaborate with the objective of saving more lives. The HFN architecture must address the needs of the individual first-responders on the ground and yet meet the challenges of a multifaceted environment. The HFN info-system architecture will not only facilitate a configurable communication network platform, but also provide an inter-exchange standard and protocol in system software applications that host a suite of select collaboration tools. The objective of this effort is to improve the communication inter-operability, effectiveness and efficiency.

The proposed implementation approach looks into the matrix of diverse scenarios, organization practices, and collaborative nature of work to make use of COTS to achieve the above objectives. Using COTS products like Central Desktop, Airwave network management tools, balloon network nodes, and the NPS research project TwiddleNet, capabilities are mixed and matched to configure a recommended solution. The research on the whole has provided an insight into examining the nature of HFN scenarios and the needs of the first-responders in HADR missions. The comprehensive architecture and the proposed implementations will benefit both DoD and DHS in preparing for improved homeland security in the future.

B. FUTURE WORK

There is some additional work that can be explored for future development. This work is related to the management of classified information and can build upon the C2 scenario developed for this thesis.

1. Multi-level Security for HFNs

Due to multi-organization participation, it was observed that the leading agencies do require multi-level security in the system to manage information control, especially the access control over classified information. Task and plan for the operation are also controlled access based on the responsibility assigned by the unified command. Such implementation will require research in a feasible security architecture that segregates information based on various factors such as roles and responsibilities and communication channel.

2. Information Assurance for HFN

A great deal of information flows thru the system with participants from multiple organizations. The need to address the information assurance in terms of confidentiality, integrity, authenticity and availability is important. There can be severely negative consequences if any of the above is compromised. Moreover, information glut is common in HADR missions, and without proper information assurance initiative, it negatively impact the decision making process. (e.g., each piece of information observed and sent to the system has to be verified and authenticated before influencing the decision plan.)

APPENDIX A – OBSERVATION REPORT FOR OPERATION GOLDEN PHOENIX TRAINING

1. INTRODUCTION

Golden Phoenix Training was held on the 16th - 26th of July by participants from local, regional, state and federal entities. The participants were involved in a collaborative civil-military operation to exercise California state and federal disaster relief protocols.

2. COLLABORATION TOOLS - C2 SYSTEMS

In this training, the Los Angeles County Police Department (LACoPD) and Los Angeles Fire Department (LAFD) fielded a new Command and Control (C2) system, the Atares System (developed by Future Systems). Apart from the C2 software applications, the complete system consists of a variety of communications connectivity to support the network between the quickly deployable Mobile Command Post (MCP) and Incident Command Post (ICP). The services that are supported by the C2 system are:

- Mapping – provides a 2D map to facilitate incident planning and situational awareness in a map view, which includes tracking of key resources
- Incident Command – provides an avenue for incident logging and updates.
- Television – provides digital broadcast of television network such as CNN
- Task – allows tracking and managing of task thru a simple process flow
- Note pad – an electronic pad for note taking.
- Internet – provides internet access

a. Observations on LACoS and LACoFD C2 System

The Atares was a new deployment (about 2-4 weeks old). Most of the participants from the two agencies were not familiar with the procedures required to record incident information. On the first two days of the training, support staff from Atares was there to provide assistance as well as on-the-job training.

With Internet access, participants were able to utilize Google Map to display their location on the map, which provided them with the awareness of the surrounding areas.

Incident command service was widely used on several occasions. It was utilized by the ground commanders to retrieve updates on the progress of the training activities. Being unfamiliar to the system, minimum collaboration work evolved around the C2 system.

b. Observations on MAG46's Content Management Web Portal (Siteframe)

MAG46 command center did not deployed its military C2 system. Innovatively, LCDR Cosby created a civil and military collaboration (www.civmil.org) portal on the internet as a platform to create situational awareness, allocation of tasks and provide regular updates of any incident.

The content management portal was easily setup using Siteframe; an open source application. It enables quick deployment of an intranet facility that allows members to share documents, pictures, diagrams and files without the hassle of much software programming. It also contains a weblog, which allows community to share information.

The key features of the Internet portal are:

- Chat – provides chat service to members of the portal.
- Map Overview – uploads a reference link of Google Earth .kmz file.
- Execution Timeline – provides timeline of events and tasking
- Training plan – presents planned scenario of GP training.

Participants from MAG46 were familiar with the portal. They were able to carry out task and perform collaboration works that were related to weblog and web chat. Application on the internet such as Google Earth was also utilized for deployment planning. The portal was hosted on the internet with simple security, such as a login ID and a password. Basically, both civil and military were able to collaborate easily using the portal.

The only drawback of the portal was the lack of processes in place to govern the flow of the portal.

c. Others Collaboration Tools

There were other collaboration tools introduced during the training, VSee and Groove. The former was an internet video conferencing tools. It had the capability to optimize transmission bandwidth and self adapt when a bandwidth resource crunch occurred. The latter was a collaboration workspace that was used by observation team to report, publish and share files.

3. COLLABORATION TOOLS - COMMUNICATIONS SYSTEMS

The communication capabilities deployed in GP were more data oriented than voice. Although radio communication in the VHF and UHF band were used during the training, it was merely used by the military and police for their intra-communication to their mobile entities. The main communication enabler was IP-based, with satellite communication equipment establishing a rear link to the public infrastructure, WiMAX APs providing the last mile communication and WAPs providing the wireless coverage to all WiFi-enabled clients within the surrounding areas. The interoperability among the command elements were supported by applications such as video-conferencing, VoIP and IP phones available in the cells.

4. MOBILE COMMAND POST

During the training, most of the agencies deployed their own MCP. It was a quick deployable “field” command centre that provided space and connectivity in the information hub.

The size and capabilities of MCP deployed ranges from a jeep to a trailer. Generally, the size can be classified into the 2 categories. The former will allow small team of 2-4 persons working from the back of the jeep. The latter is typically modeled after a command headquarter concept with working space for staff representing each functional groups and also have conference/briefing area capable to accommodate of 20-30 peoples.

Figure 1: Jeep-like CP

Figure 2: Interior of a Trailer-like MCP

Key features:

a. Mobility

With command, control and communications system integrated onto one vehicle, it provided mobility and the capability to the command center to response quickly to incident.

b. “Plug and Play”

It contains the required command and control, and communications system that enable collaboration between the ground troops. Most of the command vehicles can be deployed within 10-20 minute and it take 2-4 persons for the job.

c. “Command and Control System”

Most agencies have their own system to maintain situation awareness of the events in an incident. From the observation, most of the system looks like a “web” application riding on the internet environment. It does not seem to have a clear security separation for internet access to delineate classified information over “public” environment.

d. Communication system

The main connectivity for data communication in the MCP is facilitated by satellite communication system. Almost every MCP has own satellite dish mounted on the roof of the vehicle. On the other hand, the Motorola Tetra radio was widely used for voice communications.

Figure 3: Communication System Mounted on the Roof-top of Jeep

e. Self-sufficient power

The design of the MCP are mostly able to support itself for its power needs either thru the built in generator for those trailer type or tapping another alternate

(customized) battery supply of the vehicle. A junction box is built into each vehicle to facilitate external power source from building.

Figure 4: Customized Power Outlet on Vehicles

f. Main briefing Cell

The MCP has a main command briefing cell, where all C2 systems there are hooked up to give an overall view in terms of situation awareness.

Figure 5: Briefing Cell in a CP

5. HUMAN FACTORS

Deployment of New system – The crux of system for the main players is Antares used by both LAcoPD and LACoFD. It was no doubt that OGP provided a good environment to put the system on trial, but the participants did not seem to have knowledge or the expertise to operate the system since it is new to them too. During the interview session, we were told that the new system was delivered about a week ago. The vendor was also on site to assist the participants to enter raw data into the system. In the nutshell, more familiarity and training should be should be conducted prior to the exercise so that collaboration between participating organizations could be exercised (since one of the main objective of the OGP training was collaboration with external agencies)

Internet Culture – The proliferation of internet had unconsciously built an internet culture in our generations. From the observation of the OGP training, internet was the most common platform for information gathering and collaboration. For example, although there were map engine provided in the Antares system, but staffs from LAcoPD and MAG46 still preferred using Google Earth to perform map planning or even search for information of that area. Instant messaging was also a common tool that allowed collaboration without the need for face-to-face interaction.

Overwhelming tools and gadgets – Although most of the agencies are well equipped with system and communications devices, but it resulted in each of the agency working on their own space and connectivity – results in a seclusion problem. Another issue is the competency in using the system. In order to maximize the utilization and potential of the system, it depends greatly on the competency. However, with the growing number of gadgets and increase in functionality, it made the task more difficult to accomplish.

Conducive Environment – Most of the MCP are well built to provide the staff with an environment that was comfortable and conducive to work in. The equipment and space provided in the MCP assimilate the familiar office working environment. There were also lightning and pantry areas within the MCP.

6. OTHERS

Civil and military collaboration – MAG46 had made a significant move by using web portal on internet platform for collaboration. This made collaboration with civilian easier compared to a "close" military C2 system. Objectively the platform has greatly enables sharing and collaboration between civ-mil without much any infringement of sensitive data fear.

Governance and practices – During training, there was a clear roles and responsibilities dedicated to the main players (LAcoPD, LACoFD and MAG46). As the participants were uniformed personnel, hierarchical governance structure and practices were well defined. However, there were slight hiccups over the coordination on what tools and systems to use for collaboration for the very first time.

7. CONCLUSION

It was observed that the deployed C2 system was not put into good use in most occasions to test it interoperability, but most of organization came well prepared and equipped to function independently. The collaboration between organizations in the training still relies heavily on traditional radio communications. Interoperability was especially challenging in a multi-organization environment that even crosses civil-military boundary. In this training, system and communications interoperability were also put to test its effectiveness. For example, the Atares system was deployed for the sheriff and fire department for command and control purpose.

During the training, the participants did encounter a few interoperability hiccups, but the training had definitely provided them a good opportunity to appreciate and work together as a team in a HFN scenario – most importantly gaps were identified, lessons were learnt and good practices were put in place to better their interoperability effectiveness.

APPENDIX B – WIRELESS NETWORK CHECKLIST

WIRELESS NETWORK MANAGEMENT SYSTEM PLANNING CHECKLIST (provided by Airwave)

A Wireless Network Management System (WNMS) should enable network administrators and help-desk personnel to manage and troubleshoot an extended wireless network which serves a diverse user population who are equipped with a wide range of mobile computing devices and connect from many locations through access points that could number into the thousands.

This document provides organizations planning a wireless network with a complete checklist of the key features and capabilities they should expect to find in a wireless network management solution.

NOTE: Getting information sufficient to check a box "yes" or "no" on this list will not by itself insure that the product you choose is the right one. Competing products may both deliver a feature, yet be very different, due to the scope of the competing features, how they are achieved, how easy it is to use them, or other factors. This sheet is an initial checklist of the features you should find in a WNMS. You may need to investigate further to insure those features which are of critical importance to you deliver what you require.

General Requirements	AMP	Prod. A	Prod. B
Does it comply with all relevant IEEE and WiFi Alliance standards?			
Does it support up to thousands of wireless nodes, with the ability to manage and monitor each node individually or as part of a group?			
Does it provide a browser-based user interface (multiple browsers)?			
Does it run on standard server hardware or is it a hardware appliance.			
Does it provide different levels of management access to accommodate different support roles? Does it offer roles which both permit and deny the ability to change and/or modify device configurations?			
Can it assign different management privileges for subsets of wireless APs?			
Can each IT support user be assigned a unique user ID and password? Will actions taken by that user be logged individually for accountability?			
Is there at least nightly backup of all critical data?			
Does it provide simple restoration in the event of hardware failure?			
Does it include comprehensive help files?			

Wireless Router (AP) Discovery	AMP	Prod. A	Prod. B
A basic WNMS function is the ability to efficiently discover and assume management control over the existing wireless infrastructure and new APs and wireless controllers as they are added, without disrupting network performance.			
Does it support automatic discovery of both new and existing access points via both upper layer methods (SNMP and HTTP scanning) as well as Layer 2 discovery mechanisms (OSU-NMS, CDP, WNMP, etc.)?			
Does it provide a mechanism by which administrative users determine whether to bring a newly discovered AP under management?			
Can it import the current configuration settings from any discovered AP and automatically generate a discrepancy report highlighting any variance between the existing device configuration and pre-defined network policies?			
Does it let support users 'monitor' a newly discovered AP without applying configuration changes?			
Does it provide automated provisioning that will automatically configure any newly discovered APs to ensure compliance with network security policies?			
Can the automated provisioning feature be disabled?			

Configuration Management	AMP	Prod. A	Prod. B
A WNMS must give network administrators the ability to define central network configuration policies and apply those policies across the entire wireless network infrastructure, covering access point and router hardware from multiple vendors.			
Does it support configuration of wireless access points from many leading hardware vendors, or only one vendor? A*ttach a complete matrix of all AP makes, models, and firmware versions which are supported. Does it support:*			
• Cisco Aironet/Airespace			
• Aruba Networks			
• Symbol			
• Proxim			
• ProCurve by HP			
• Enterasys			
• Avaya			
• Colubris Networks			
• Nomadix			
• LANCOM Systems			
• Intermec			
• Dell			
• 3Com			
• Other _____			
• Can it manage all APs from one common user interface?			
• Does it permit configuration of variable settings on supported APs?			
• Does it support configuration of 802.11b, 802.11g, and 802.11a APs?			
• Does it support all major configuration protocols, including:			
• SNMPv1			

• SNMPv2			
• SNMPv3			
• HTTP			
• HTTPS			
• Telnet/CLI			
• SSH/CLI			
Does it permit implementing configuration changes globally to all APs, to specified "groups" or subsets of APs, or to an individual AP?			
After making configuration changes, can it verify that the change(s) have been successfully implemented?			
Can administrative users define 'groups' of APs (up to 1000 groups) by any location, function, brand, etc. for distributed management and monitoring?			
Is there support multiple encryption modes, including the following:			
• WEP			
• WEP+802.1x			
• LEAP			
• LEAP+802.1x			
• WPA			
• WPA/PSK			
Does it permit different encryption modes to be implemented on different subsets of wireless APs?			
Does it support configuration and monitoring of wireless access points with two radios? Can each radio be configured independently?			
Can it configure multiple VLANs and SSIDs per wireless access point? Can it apply all supported encryption modes to any VLAN/SSID?			
Can it apply a configuration change immediately and at a scheduled time?			
Can it configure wireless APs behind NAT gateways?			
Can it provide protocol port mapping on a per AP basis for any AP behind a gateway?			
Can it provide a full audit trail for all configuration changes, including user and date/time?			

Audit Management & Policy Enforcement	**AMP**	**Prod. A**	**Prod. B**
Because a major threat to wireless security comes from misconfigured and unconfigured access points, a WNMS must be able to audit the configuration of the wireless network infrastructure on an ongoing basis, identifying any devices that do not comply with policies, and take automatic corrective action.			
Does it audit all managed wireless access point to ensure that configuration and encryption settings comply with centrally defined policies?			
Can it conduct configuration audits at scheduled intervals? Can this function be disabled to reduce network traffic if desired?			
Does it display onscreen a report specifying exact AP configuration settings that do not comply with predefined policies?			
Does it automatically repair any AP configurations not in compliance?			
Can it provide inventory reports and other information to assist with Sarbanes-Oxley compliance, if required?			

Network & User Monitoring	AMP	Prod. A	Prod. B
Day to day, the chief function of a WNMS is to gather, display, and analyze real-time performance information from the wireless network which will enable the operator to handle problems, monitor performance, and manage all elements.			
Does it display a 'dashboard' with real-time wireless network use information including:			
# of managed devices			
# of connected users			
# of alerts			
# of unauthorized rogue devices			
Cumulative bandwidth usage			
Does it collect, analyze and display real-time and historical data from every AP, including:			
# of connected clients			
Bandwidth utilization			
AP make/model			
AP firmware version			
"dot11" Counters			
Is all information graphically represented?			
Does it include a user/device 'search' function to allow support users to quickly locate any device or user on the network?			
Does it recognize and report client device roaming patterns, including APs used, connection time per AP, and failed roaming attempts?			
Does it collect, analyze and display both real-time and historical performance data from every connected client, including:			
Bandwidth utilization,			
RF signal quality			
Authentication status/time			
AP roaming patterns			
Connection time and duration			
"First seen/Last seen" date/time			
Username			
MAC address			
IP address			
Device vendor			
Can it support configurable polling intervals and SNMP timeout/retries to ensure proper functioning, even in high-latency environments?			
Can polling intervals vary among different groups of APs?			
Does it include a radio frequency (RF) visualization function?			
Does the RF visualization function allow the support user to see:			
Real-time RF coverage areas			
RF 'heat maps'			
Client/user location			
Channel maps			

Rogue Access Point Detection	AMP	Prod. A	Prod. B
The WNMS must provide a reliable, accurate way to detect rogue APs which also minimizes 'false positive' results. Must be able to detect rogue APs without reliance on separate hardware RF sensors or probes.			
Can it automatically detect unauthorized 'rogue' access points using existing, managed APs to conduct RF scans?			
Can it use wired network discovery techniques to detect rogue APs that are not within range of any other APs or wireless sensors?			
Does it include filtering or 'scoring' mechanisms to distinguish benign from hostile rogues and to minimize 'false positives?'			
Does it have a way (i.e., client software for WiFi devices) to wirelessly detect rogue APs out of range of existing APs without sensors or probes?			
Can it locate rogue APs and identify the port the rogue is connected to?			
Does it include a rogue location function that triangulates the likely physical location of the rogue device, using all available RF data?			
Does it provide the following to assist in locating any discovered rogue APs?			
SSID			
RSSI (Signal Strength)			
WEP Bit			
IP Address			
MAC address			
LAN MAC			
Switch & port			
Can it show how and when the rogue AP was discovered?			
Can it differentiate between ad-hoc and infrastructure network devices?			
Is it able to stop reporting about devices determined not to be a threat?			

Firmware Distribution & Management	AMP	Prod. A	Prod. B
Wireless network hardware manufacturers are regularly updating the firmware on their devices. A WNMS must automatically update firmware on wireless LAN infrastructure devices and verify successful completion of the updates.			
Does it support all protocols required (tftp, SNMP, HTTP, etc.) which allow firmware to be remotely upgraded on all supported makes and models of AP?			
Can it store and catalog firmware versions by make and model of AP?			
Are users able to define a 'minimum acceptable' firmware version for each make and model of AP supported?			
Can it automatically detect and update any APs with 'down-rev' firmware?			
Can it determine new and deprecated settings between firmware versions and automatically reconfigure APs to comply with group configuration policies when upgrading or downgrading firmware?			
Will it allow firmware upgrades to be scheduled for any time of the day?			
Can it perform system verification prior to any scheduled firmware or operating system upgrade to ensure that the upgrade will be successful?			
Can it validate than a firmware or OS upgrade has been successful?			
In the case of upgrade failure during a scheduled group upgrade, can the WNMS detect the failure, stop the group upgrade process, and alert an administrator? (Function required even if an external tftp server is utilized.)			

Diagnostics & Alerts	AMP	Prod. A	Prod. B
A WNMS is used to diagnose, assign severity codes, and alert IT staff when problems occur that may impact users or network performance. It should provide sufficient information and controls to permit efficient resolution.			
Can it automatically generate the following alarms on a 24x7 basis:			
Deviation from security/configuration policies (misconfigured AP)			
New APs discovered			
Rogue wireless networks or APs discovered			
Overlapping RF channel assignments detected			
Excessive AP usage (bandwidth or connected clients)			
Excessive bandwidth usage by individual clients			
'Down' (unmanageable) APs,			
Is there a clearly visible link to all unresolved alerts throughout the UI?			
Can support users assign a severity code for every type of alert?			
Can it filter alerts by severity code?			
Can users acknowledge and/or delete alarms in the WNMS user interface?			
Will it deliver alerts via email, console, and through traps to existing Fault Management Systems (such as HP OpenView)?			

Trend Reporting	AMP	Prod. A	Prod. B
The WNMS must report on performance, current use patterns, identify potential areas of vulnerability, and deliver a full set of exportable performance reports that can cover both current and historical data in graphical form.			
Must provide at minimum the following reports:			
Access Point Inventory Report (listing all devices on the WLAN)			
Client Session Report (listing each individual client session, duration, and cumulative bandwidth usage)			
Network Usage Report (WLAN usage by time of day)			
Most/Least Utilized AP Report			
Uptime Report (Uptime by AP)			
Is all data from the WNMS reports exportable?			
Can the WNMS reports be customized to run for specified groups of APs and/or for specified periods of time?			
Can use and performance data be retained for a year or more?			
Can it automatically email reports to a distribution list on a defined schedule?			

Dynamic RF Management	AMP	Prod. A	Prod. B
Must assist the IT staff in identifying and resolving RF issues on the fly and provide IT full control over the RF settings on all WiFi infrastructure devices.			
Does it automatically identify when contiguous APs (including rogue and/or neighboring APs) are assigned to the same RF channel?			
Can it support configuration of AP channel and transmission power settings?			
Does it optimize and automate the selection of RF channels?			

Does it display 'before' and 'after' channel maps for administrator review and approval prior to activation?			
Does it provide real-time data and historical trend reports on 802.11 counters for RF trouble-shooting (including RF transmission errors, data rates, etc.)?			

Wireless Network Provisioning and RF Planning	AMP	Prod. A	Prod. B
The WNMS should provide an easy-to-learn design tool that interoperates with the WNMS and automates the device configuration process.			
Dos it include a graphical wireless site planning tool to assist in the location and RF configuration wireless APs?			
Can it import maps in any major format (JPEG, CAD, Visio, etc.)?			
Can it automatically calculate estimated RF coverage areas based on the make/model of access point, antenna type, RF transmission power, etc.?			
Will it interoperate with the site planning tool to enable AP settings specified in the site plan to be automatically implemented when APs are discovered.			

Training, Documentation & Support	AMP	Prod. A	Prod. B
Will the vendor provide on-site training sufficient to enable self-support and operation?			
Will books and other class materials be included?			
Will vendor certification costs, if any, be born by the contractor?			
Will the vendor provide documentation in electronic format (Adobe PDF)?			
Will the vendor provide technical support and software maintenance?			
Is technical support available by phone, web, and/or e-mail?			
What is covered and what is the cost of the vendor's maintenance program?			

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

[1] Paul A Pavlou, Angelika Dimoka, Thomas J Housel, The MOVES Institute, Collaborative IT Tools Leveraging Competence in Hastily Formed Network. Proceedings in HFN Brown Bag. Available from http://www.hfncenter.org/cms/ITTools, last accessed 21 Jun 2007.

[2] Net-Centric Enterprise Services (NCES) Defense Information Systems Agency Website. Available from http://www.disa.mil/nces/product_lines/collaboration.html, last accessed 26Aug 2007.

[3] Peter Denning, Hastily Formed Networks, Communications of ACM (April 2006/Vol. 49 No. 4). Available from http://www.nps.edu/Cebrowski/Docs/cacmApr06.pdf, last accessed 3 Sep 2007.

[4] Michael Sampson, Collaboration Success Advisors Ltd, A six step for achieving collaboration success and improving business with Central Desktop (June 2007). Available from http://www.centraldesktop.com/collaboration_whitepaper, last accessed 28 Aug 2007.

[5] Lizbeth Goodman and Katherine Milton, A Guide to Good Practice in Collaborative Tools and New Media Tools Creation. (June 2007). Available from http://ahds.ac.uk/creating/guides/new-media-tools/, last accessed 4 July 2007.

[6] Ed Ort, Service Oriented Architecture and Web Services – Concept, Technologies and Tools, Whitepaper by Sun Microsystems (Apr 2005). Available from http://java.sun.com/developer/technicalArticles/WebServices/soa2/, last accessed 14 Oct 2007.

[7] Debbie Stone, Caroline Jarrett, Mark Woodroffe, Shailey Minocha, User Interface Design and Evaluation. Morgan Kaufmann, 2005.

[8] IT Transformation to Service Oriented Architecture Technical White Paper (May 2004). Available from http://www.bea.com/content/news_events/white_papers/BEA_SOA_Transformation_WP.pdf , last accessed 4 Jun 2007.

[9] B.S. Manoj, Alexandra Hubenko Baker, Communications challenge in emergency response (Communications of ACM, March 2007, Vol 50 No. 3). Available from http://delivery.acm.org/10.1145/1230000/1226765/p51-manoj.pdf?key1=1226765&key2=7980146911&coll=GUIDE&dl=GUIDE&CFID=45174112&CFTOKEN=29985676, last accessed 10 Aug 2007.

[10] Steve Sawyer, Andrea Tapia, Leonard Pesheck, John Davenport, Mobility and First responders (Communications of ACM, March 2004, Vol 47 No. 3). Available from

http://delivery.acm.org/10.1145/980000/971647/p62-sawyer.pdf?key1=971647&key2=2611146911&coll=GUIDE&dl=GUIDE&CFID=45174340&CFTOKEN=32638766, last accessed 20 Aug 2007.

[11] Brian Steckler, Bryan L. Bradford, Steve Urrea, After Action Report and Lesson Learned from NPS's Response to Hurricane Katrina. Available from http://www.nps.navy.mil/DisasterRelief/docs/NPS-Katrina_AAR_LL.pdf, last accessed 15 Jun 2007.

[12] George S. Ake, Capital Wireless Integrated Network (CapWIN): Building a Bridge in Transportation and Public Safety Communications. Available from http://diggov.org/library/library/dgo2005/invitedtalks/capwin.pdf, last accessed 21 Jul 2007.

[13] Viktor Mayer-Schönberger, The Challenging Interface of Technology and Policy: A Case Study of Communications Interoperability (Proceedings of the 2003 annual national conference on Digital government research, 2003, Vol 130). Available from http://delivery.acm.org/10.1145/1130000/1123298/p101-mayer-schonberger.pdf?key1=1123298&key2=1871146911&coll=GUIDE&dl=GUIDE&CFID=45175051&CFTOKEN=72518502, last accessed 9 Aug 2007.

[14] David. D Lancaster, Developing a Fly-Away-Kit (FLAK) to Support Hastily Formed Networks (HFN) for Humanitarian Assistance and Disaster Relief (HA/DR). Available from http://stinet.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA435513, last accessed 24 Aug 2007.

[15] The Strong Angel Team, Stability, Security, Transition, and Reconstruction. Observations and Recommendations from the Field. Available from http://www.strongangel3.net/files/sstr_20061107_web.pdf, last accessed 24 Aug 2007.

[16] Bill Murray, HFN Brown Bag: Essential Security Practices for Hastily Formed Network (2007). Available from www.nps.edu/cebrowski/Docs/HFN%20Security.ppt, last accessed 25 Aug 2007.

[17] Intel, Understanding WiFi and WiMAX as Metro-Access Solutions, Whitepaper by Intel (2004). Available from http://www.intel.com/netcomms/technologies/wimax/304471.pdf, last accessed 20 Oct 2007.

[18] Bryan L. Bradford, Wireless Security Within Hastily Formed Networks. Available from http://stinet.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA456940, last accessed 21 Oct 2007.

[19] Airwave Wireless Inc, Airwave Wireless Management Suite 5.0 Solution Guide (2006). Available from http://airwave.com/docs/brochures/airwave-solution-guide-5-0.pdf, last accessed 29 Oct 2007.

[20] Hurricane Katrina. Available from http://en.wikipedia.org/wiki/Hurricane_katrina, last read 12 Oct 2007.

[21] Brian Steckler, Hastily Formed Networks (HFN) Defined Presentation Slides (12 Dec 2006). Available from http://www.wca.org/backup/eclic_pastmeetings/STECKLER_eCLIC_12Dec06.ppt, last accessed 15 July 2007.

[22] Peter J. Denning and Rick Hayes-Roth Decision Making in Very Large Networks (Communications of ACM, November 2006, Vol 49 No. 11). Available from http://cs.gmu.edu/cne/pjd/PUBS/CACMcols/cacmNov06.pdf, last accessed 11 Aug 2007.

[23] Department of Defense Directive, Military Support for Stability, Security, Transition, and Reconstruction (SSTR) Operations (November 2005). Available from http://www.dtic.mil/whs/directives/corres/pdf/300005p.pdf, last accessed 23 Aug 2007.

[24] GSM Association, The Role of Mobiles in Disasters and Emergencies (December 2005). Available from http://www.vodafone.com/etc/medialib/attachments/cr_downloads.Par.2217.File.tmp/GSM_Report.pdf, last accessed 23 July 2007.

[25] Gurminder Singh (2007) TwiddleNet: Immediate Content Capture and Dissemination for First Responders. Workshop on Mobile HCI for Emergencies, 9 Sep 2007, Singapore.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Prof. Yeo Tat Soon
   Directory Of Temasek Defence System Institute
   National University of Singapore
   Singapore

4. Tan Lai Poh
   National University of Singapore
   Singapore

5. Ng Min Yew Calvin
   FMS students: Civilian, Naval Postgraduate School
   Monterey, California

6. Lim Meng Hwee
   FMS students: Civilian, Naval Postgraduate School
   Monterey, California